



Panduan Pengguna Hooks

CloudFormation



CloudFormation: Panduan Pengguna Hooks

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu CloudFormation Hooks?	1
Opsi implementasi kait	1
AWS Control Tower kontrol proaktif	1
Aturan penjaga	1
Fungsi Lambda	2
Kait Kustom	2
Membuat dan mengelola Hooks	3
Konsep	5
Kait	6
Mode kegagalan	6
Target kait	6
Tindakan target	7
Anotasi	7
Handler kait	7
Batas batas waktu dan coba lagi	8
Kontrol proaktif sebagai Hook	8
AWS CLI perintah untuk bekerja dengan Hooks	9
Aktifkan Hook berbasis kontrol proaktif	9
Hapus Hooks berbasis kontrol proaktif	13
Kait Pelindung	14
AWS CLI perintah untuk bekerja dengan Guard Hooks	15
Tulis aturan Guard untuk Hooks	15
Bersiaplah untuk membuat Guard Hook	29
Aktifkan Guard Hook	31
Lihat log untuk Guard Hooks	37
Hapus Guard Hooks	37
Kait Lambda	38
AWS CLI perintah untuk bekerja dengan Lambda Hooks	39
Buat fungsi Lambda untuk Hooks	39
Bersiaplah untuk membuat Lambda Hook	63
Aktifkan Lambda Hook	65
Lihat log untuk Lambda Hooks	70
Hapus Lambda Hooks	70
Kait Kustom	72

Prasyarat	73
Memulai proyek Hooks	75
Kait Pemodelan	78
Mendaftarkan Hooks	145
Pengujian Kait	150
Memperbarui Hooks	159
Deregistering Hooks	160
Kait Penerbitan	160
Skema sintaks	169
Nonaktifkan-mengaktifkan Hooks	178
Nonaktifkan dan aktifkan Hook (konsol)	178
Nonaktifkan dan aktifkan Hook (AWS CLI)	178
Lihat hasil pemanggilan Hook	180
Lihat hasil pemanggilan (konsol)	180
Lihat hasil untuk semua Hooks	180
Lihat riwayat pemanggilan untuk masing-masing Hooks	181
Lihat hasil untuk pemanggilan khusus tumpukan	181
Lihat hasil pemanggilan ()AWS CLI	182
Skema konfigurasi	187
Properti skema konfigurasi kait	187
Contoh konfigurasi kait	189
Filter tingkat tumpukan	189
FilteringCriteria	191
StackNames	191
StackRoles	192
Include dan Exclude	193
Contoh filter tingkat tumpukan	193
Filter target	197
Contoh filter target	199
Menggunakan wildcard	201
Buat Hooks menggunakan template CloudFormation	210
Berikan izin IAM	212
Izinkan pengguna untuk mengelola Hooks	213
Izinkan pengguna untuk mempublikasikan Hooks kustom secara publik	214
Izinkan pengguna untuk melihat hasil pemanggilan Hook	215
Daftar hasil pemanggilan Hook	215

Izinkan pengguna untuk melihat hasil pemanggilan Hook yang terperinci	218
AWS KMS kebijakan dan izin utama	219
Ikhtisar	219
Konteks enkripsi	220
Kebijakan kunci KMS yang dikelola pelanggan	221
Izin KMS untuk API SetTypeConfiguration	224
Izin KMS untuk API GetHookResult	225
Riwayat dokumen	226
.....	CCXXX

Apa itu CloudFormation Hooks?

CloudFormation Hooks adalah fitur yang membantu memastikan bahwa CloudFormation sumber daya, tumpukan, dan set perubahan Anda mematuhi praktik terbaik keamanan, operasional, dan pengoptimalan biaya organisasi Anda. CloudFormation Hooks juga dapat memastikan tingkat kepatuhan yang sama untuk AWS Cloud Control API sumber daya Anda. Dengan CloudFormation Hooks, Anda dapat memberikan kode yang secara proaktif memeriksa konfigurasi AWS sumber daya Anda sebelum penyediaan. Jika sumber daya yang tidak sesuai ditemukan, CloudFormation operasi gagal dan mencegah sumber daya disediakan atau memancarkan peringatan dan memungkinkan operasi penyediaan dilanjutkan.

Anda dapat menggunakan Hooks untuk menerapkan berbagai persyaratan dan pedoman. [Misalnya, Hook terkait keamanan dapat memverifikasi bahwa grup keamanan memiliki peraturan lalu lintas masuk dan keluar yang sesuai untuk VPC Amazon Anda.](#) Hook terkait biaya dapat membatasi lingkungan pengembangan untuk hanya menggunakan jenis instans [Amazon EC2](#) yang lebih kecil. [Hook yang dirancang untuk ketersediaan data dapat menerapkan pencadangan otomatis untuk Amazon RDS.](#)

Opsi implementasi kait

CloudFormation menyediakan beberapa opsi untuk menerapkan Hooks, memberi Anda fleksibilitas untuk memilih pendekatan yang paling sesuai dengan kebutuhan Anda.

AWS Control Tower kontrol proaktif

Katalog AWS Control Tower Kontrol menawarkan kontrol proaktif standar yang dapat Anda terapkan sebagai Hooks. Pendekatan ini menghemat waktu persiapan dan membantu Anda memvalidasi konfigurasi sumber daya terhadap praktik AWS terbaik di seluruh organisasi Anda tanpa menulis kode.

Aturan penjaga

AWS CloudFormation Guard adalah alat policy-as-code evaluasi yang menyediakan bahasa khusus domain untuk menulis logika evaluasi khusus untuk Hooks. Pendekatan ini memungkinkan Anda untuk menentukan pemeriksaan kepatuhan menggunakan sintaks deklaratif Guard, sehingga mudah untuk membuat dan memelihara logika evaluasi Anda tanpa pengetahuan pemrograman yang luas.

Fungsi Lambda

Anda juga dapat menerapkan Hooks menggunakan fungsi Lambda, memungkinkan Anda untuk memanfaatkan kekuatan penuh dan fleksibilitas Lambda untuk logika evaluasi Anda. Anda dapat menggunakan bahasa runtime yang didukung Lambda dan berintegrasi dengan AWS layanan lain sesuai kebutuhan.

Kait Kustom

Untuk kasus penggunaan lanjutan, Anda dapat menulis logika evaluasi Anda sendiri menggunakan bahasa pemrograman yang didukung oleh [CloudFormation CLI](#). Pendekatan ini memberikan fleksibilitas maksimum untuk menerapkan persyaratan tata kelola khusus organisasi. Sebagai jenis ekstensi yang didukung dalam [CloudFormation registri](#), Hooks kustom Anda dapat didistribusikan dan diaktifkan baik secara publik maupun pribadi.

Membuat dan mengelola CloudFormation Hooks

CloudFormation Hooks menyediakan mekanisme untuk mengevaluasi CloudFormation sumber daya Anda sebelum mengizinkan pembuatan tumpukan, modifikasi, atau penghapusan. Fitur ini membantu Anda memastikan bahwa CloudFormation sumber daya Anda mematuhi praktik terbaik keamanan, operasional, dan pengoptimalan biaya organisasi Anda.

Untuk membuat Hook, Anda memiliki empat opsi.

- Kontrol proaktif sebagai Hooks — Mengevaluasi sumber daya menggunakan kontrol proaktif dari Katalog Kontrol. AWS Control Tower
- Guard Hook — Mengevaluasi sumber daya menggunakan AWS CloudFormation Guard aturan.
- Lambda Hook — Meneruskan permintaan untuk evaluasi sumber daya ke suatu fungsi. AWS Lambda
- Custom Hook - Menggunakan handler Hook kustom yang Anda kembangkan secara manual.

Proactive controls as Hooks

Untuk membuat Hook dari kontrol proaktif, ikuti langkah-langkah berikut:

1. Arahkan ke CloudFormation konsol dan mulailah membuat Hook.
2. Pilih kontrol tertentu dari Katalog Kontrol yang ingin Anda evaluasi terhadap sumber daya Hook Anda.

Kontrol ini akan secara otomatis berlaku setiap kali sumber daya tertentu dibuat atau diperbarui. Pilihan Anda menentukan jenis sumber daya mana yang akan dievaluasi oleh Hook.

3. Setel mode Hook untuk memperingatkan pengguna tentang ketidakpatuhan atau mencegah operasi yang tidak sesuai.
4. Konfigurasi filter opsional untuk menyertakan atau mengecualikan tumpukan berdasarkan nama tumpukan atau peran tumpukan.
5. Setelah menyelesaikan konfigurasi, aktifkan Hook untuk memulai penegakan hukum.

Guard Hook

Untuk membuat Guard Hook, ikuti langkah-langkah berikut:

1. Tulis logika evaluasi sumber daya Anda sebagai aturan kebijakan Guard menggunakan Guard domain-specific language (DSL).
2. Simpan aturan kebijakan Penjaga di bucket Amazon S3.
3. Arahkan ke CloudFormation konsol dan mulailah membuat Guard Hook.
4. Berikan jalur Amazon S3 ke aturan Penjaga Anda.
5. Pilih jenis target spesifik yang akan dievaluasi oleh Hook.
 - CloudFormation sumber daya (RESOURCE)
 - Seluruh template tumpukan (STACK)
 - Ubah set (CHANGE_SET)
 - Sumber daya Cloud Control API (CLOUD_CONTROL)
6. Pilih tindakan penerapan (buat, perbarui, hapus) yang akan memanggil Hook Anda.
7. Pilih bagaimana Hook merespons ketika gagal evaluasi.
8. Konfigurasi filter opsional untuk menentukan jenis sumber daya mana yang harus dievaluasi oleh Hook
9. Konfigurasi filter opsional untuk menyertakan atau mengecualikan tumpukan berdasarkan nama tumpukan atau peran tumpukan.
10. Setelah menyelesaikan konfigurasi, aktifkan Hook untuk memulai penegakan hukum.

Lambda Hook

Untuk membuat Lambda Hook, ikuti langkah-langkah berikut:

1. Tulis logika evaluasi sumber daya Anda sebagai fungsi Lambda.
2. Arahkan ke CloudFormation konsol dan mulailah membuat Lambda Hook.
3. Berikan Nama Sumber Daya Amazon (ARN) untuk fungsi Lambda Anda.
4. Pilih jenis target spesifik yang akan dievaluasi oleh Hook.
 - CloudFormation sumber daya (RESOURCE)
 - Seluruh template tumpukan (STACK)
 - Ubah set (CHANGE_SET)
 - Sumber daya Cloud Control API (CLOUD_CONTROL)
5. Pilih tindakan penerapan (buat, perbarui, hapus) yang akan memanggil Hook Anda.

6. Pilih bagaimana Hook merespons ketika gagal evaluasi.
7. Konfigurasi filter opsional untuk menentukan jenis sumber daya mana yang harus dievaluasi oleh Hook
8. Konfigurasi filter opsional untuk menyertakan atau mengecualikan tumpukan berdasarkan nama tumpukan atau peran tumpukan.
9. Setelah menyelesaikan konfigurasi, aktifkan Hook untuk memulai penegakan hukum.

Custom Hook

Custom Hooks adalah ekstensi yang Anda daftarkan di CloudFormation registri menggunakan CloudFormation Command Line Interface (CFN-CLI).

Untuk membuat Hook kustom, ikuti langkah-langkah utama berikut:

1. Memulai proyek — Menghasilkan file yang diperlukan untuk mengembangkan Hook kustom.
2. Model Hook — Tulis skema yang mendefinisikan Hook dan penanganan yang menentukan operasi yang dapat memanggil Hook.
3. Daftarkan dan aktifkan Hook — Setelah Anda membuat Hook, Anda harus mendaftarkannya di akun dan Wilayah tempat Anda ingin menggunakannya dan ini mengaktifkannya.

Topik berikut memberikan informasi lebih lanjut untuk membuat dan mengelola Hooks.

Topik

- [CloudFormation Konsep kait](#)
- [AWS Control Tower kontrol proaktif sebagai Hooks](#)
- [Kait Pelindung](#)
- [Kait Lambda](#)
- [Mengembangkan Hooks kustom menggunakan CLI CloudFormation](#)

CloudFormation Konsep kait

Terminologi dan konsep berikut sangat penting untuk pemahaman Anda dan penggunaan CloudFormation Hooks.

Kait

Hook berisi kode yang dipanggil segera sebelum CloudFormation membuat, memperbarui, atau menghapus tumpukan atau sumber daya tertentu. Hal ini juga dapat dipanggil selama operasi membuat perubahan set. Hooks dapat memeriksa template, sumber daya, atau set perubahan yang akan CloudFormation disediakan. Selain itu, Hooks dapat dipanggil segera sebelum [Cloud Control API](#) membuat, memperbarui, atau menghapus sumber daya tertentu.

Jika Hook mengidentifikasi konfigurasi apa pun yang tidak sesuai dengan pedoman organisasi yang ditentukan dalam logika Hook Anda, maka Anda dapat memilih salah satu WARN pengguna atau FAIL, CloudFormation mencegah penyediaan sumber daya.

Kait memiliki karakteristik sebagai berikut:

- Validasi proaktif — Mengurangi risiko, overhead operasional, dan biaya dengan mengidentifikasi sumber daya yang tidak sesuai sebelum dibuat, diperbarui, atau dihapus.
- Penegakan otomatis — Menyediakan penegakan hukum dalam Akun AWS diri Anda untuk mencegah sumber daya yang tidak sesuai disediakan oleh CloudFormation

Mode kegagalan

Logika Hook Anda dapat mengembalikan kesuksesan atau kegagalan. Respons yang sukses akan memungkinkan operasi berlanjut. Kegagalan sumber daya yang tidak sesuai dapat mengakibatkan hal berikut:

- FAIL- Menghentikan operasi penyediaan.
- WARN— Memungkinkan penyediaan untuk melanjutkan dengan pesan peringatan.

Membuat Hooks dalam WARN mode adalah cara yang efektif untuk memantau perilaku Hook tanpa memengaruhi operasi tumpukan. Pertama, aktifkan Hooks dalam WARN mode untuk memahami operasi mana yang akan terpengaruh. Setelah Anda menilai efek potensial, Anda dapat mengalihkan FAIL mode Hook ke untuk mulai mencegah operasi yang tidak sesuai.

Target kait

Target hook menentukan operasi yang akan dievaluasi oleh Hook. Ini bisa berupa operasi pada:

- Sumber daya yang didukung oleh CloudFormation (RESOURCE)

- Template tumpukan (STACK)
- Ubah set (CHANGE_SET)
- Sumber daya yang didukung oleh [Cloud Control API](#) (CLOUD_CONTROL)

Anda menentukan satu atau lebih target yang menentukan operasi terluas yang akan dievaluasi oleh Hook. Misalnya, Anda dapat membuat penargetan Hook RESOURCE untuk menargetkan semua AWS sumber daya dan STACK menargetkan semua templat tumpukan.

Tindakan target

Tindakan target menentukan tindakan tertentu (CREATE, UPDATE, atau DELETE) yang akan memanggil Hook. Untuk RESOURCE, STACK, dan CLOUD_CONTROL target, semua tindakan target dapat diterapkan. Untuk CHANGE_SET target, hanya CREATE tindakan yang berlaku.

Anotasi

[GetHookResult](#) tanggapan dapat mengembalikan anotasi yang memberikan hasil pemeriksaan kepatuhan terperinci dan panduan remediasi untuk setiap sumber daya yang dievaluasi. Untuk detail tentang struktur anotasi API, lihat [Anotasi di Referensi AWS CloudFormation API](#). Untuk petunjuk tentang melihat hasil validasi ini, lihat [Lihat hasil pemanggilan untuk Hooks CloudFormation](#).

Anda dapat mengenkripsi anotasi sesuai kebutuhan untuk informasi kepatuhan sensitif dengan menentukan kunci KMS Anda sendiri saat mengonfigurasi Hook. Untuk informasi selengkapnya, lihat [Referensi sintaks skema konfigurasi hook](#). Untuk informasi tentang menyiapkan kebijakan kunci yang Anda perlukan saat menentukan kunci KMS untuk Hooks, lihat [AWS KMS kebijakan kunci dan izin untuk mengenkripsi hasil CloudFormation Hooks saat istirahat](#)

Important

Perhatikan bahwa KmsKeyId opsi untuk menentukan kunci yang dikelola pelanggan saat ini hanya tersedia saat Anda menggunakan tombol AWS CLI untuk mengonfigurasi Hook Anda.

Handler kait

Untuk Hooks kustom, ini adalah kode yang menangani evaluasi. Ini terkait dengan titik pemanggilan target dan tindakan target yang menandai titik yang tepat di mana Hook berjalan. Anda menulis penanganan yang menjadi tuan rumah logika untuk poin-poin spesifik ini. Misalnya, titik pemanggilan

PRE target dengan tindakan CREATE target membuat handler preCreate Hook. Kode dalam handler Hook berjalan ketika titik pemanggilan target yang cocok dan layanan melakukan tindakan target terkait.

Nilai yang valid: (preCreate|preUpdate|preDelete)

Important

Operasi tumpukan yang menghasilkan status UpdateCleanup jangan memanggil Hook. Misalnya, selama dua skenario berikut, preDelete handler Hook tidak dipanggil:

- tumpukan diperbarui setelah menghapus satu sumber daya dari template.
- sumber daya dengan jenis [penggantian](#) pembaruan dihapus.

Batas batas waktu dan coba lagi

Hooks memiliki batas waktu tunggu 30 detik per pemanggilan dan dibatasi hingga 3 upaya coba lagi. Jika pemanggilan melebihi batas waktu, kami mengembalikan pesan kesalahan yang menyatakan bahwa eksekusi Hook habis waktu. Setelah percobaan ulang ketiga, CloudFormation tandai eksekusi Hook sebagai gagal.

AWS Control Tower kontrol proaktif sebagai Hooks

Katalog AWS Control Tower Kontrol menyediakan aturan kepatuhan bawaan (kontrol proaktif) yang dapat Anda terapkan sebagai Hooks. Pendekatan ini menghemat waktu penyiapan dan membantu Anda memvalidasi konfigurasi sumber daya terhadap praktik AWS terbaik di seluruh organisasi Anda tanpa menulis kode.

Kontrol proaktif mengevaluasi AWS sumber daya sebelum penerapan, mencegah sumber daya yang tidak sesuai dibuat daripada mendeteksi masalah nanti. Mereka memeriksa konfigurasi terhadap standar keamanan, operasional, dan tata kelola yang ditetapkan.

Untuk memulai, cukup aktifkan Hooks berbasis kontrol proaktif di akun dan Wilayah yang Anda inginkan. Hooks ini kemudian akan mengevaluasi jenis target tertentu untuk memastikan kepatuhan dengan kontrol yang Anda pilih.

Untuk informasi selengkapnya tentang kontrol proaktif yang tersedia, lihat [Katalog AWS Control Tower Kontrol](#).

Topik

- [AWS CLI perintah untuk bekerja dengan Hooks](#)
- [Aktifkan Hook berbasis kontrol proaktif di akun Anda](#)
- [Hapus Hooks berbasis kontrol proaktif di akun Anda](#)

AWS CLI perintah untuk bekerja dengan Hooks

AWS CLI Perintah untuk bekerja dengan Hooks berbasis kontrol proaktif meliputi:

- [activate-type](#) untuk memulai proses aktivasi untuk Hook berbasis kontrol proaktif.
- [set-type-configuration](#) untuk menentukan kontrol yang akan diterapkan ke Hook berbasis kontrol proaktif di akun Anda.
- [list-types](#) untuk mencantumkan Hooks di akun Anda.
- [describe-type](#) untuk mengembalikan informasi terperinci tentang Hook tertentu atau versi Hook tertentu, termasuk data konfigurasi saat ini.
- [deactivate-type](#) untuk menghapus Hook yang sebelumnya diaktifkan dari akun Anda.

Aktifkan Hook berbasis kontrol proaktif di akun Anda

Topik berikut menunjukkan kepada Anda cara mengaktifkan Hook berbasis kontrol proaktif di akun Anda, yang membuatnya dapat digunakan di akun dan Wilayah tempat pengaktifannya.

Important

Sebelum melanjutkan, verifikasi bahwa Anda memiliki izin yang diperlukan untuk bekerja dengan Hooks dan melihat kontrol proaktif dari konsol. CloudFormation Untuk informasi selengkapnya, lihat [Berikan izin IAM untuk Hooks CloudFormation](#).

Topik

- [Aktifkan Hook berbasis kontrol proaktif \(konsol\)](#)
- [Aktifkan Hook \(\) berbasis kontrol proaktif AWS CLI](#)

Aktifkan Hook berbasis kontrol proaktif (konsol)

Untuk mengaktifkan Hook berbasis kontrol proaktif untuk digunakan di akun Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Anda ingin membuat Hook.
3. Di panel navigasi di sebelah kiri, pilih Hooks.
4. Pada halaman Hooks, pilih Create a Hook, lalu pilih With the Control Catalog.
5. Pada halaman Pilih kontrol, untuk kontrol Proaktif, pilih satu atau beberapa kontrol proaktif untuk digunakan.

Kontrol ini akan secara otomatis berlaku setiap kali sumber daya tertentu dibuat atau diperbarui. Pilihan Anda menentukan jenis sumber daya mana yang akan dievaluasi oleh Hook.

6. Pilih Berikutnya.
7. Untuk nama Hook, pilih salah satu opsi berikut:
 - Berikan nama deskriptif singkat yang akan ditambahkan setelahnya `Private::Controls::`. Misalnya, jika Anda masuk *MyTestHook*, nama Hook lengkap menjadi `Private::Controls::MyTestHook`.
 - Berikan nama Hook lengkap (juga disebut alias) menggunakan format ini: `Provider::ServiceName::HookName`.
8. Untuk mode Hook, pilih bagaimana Hook merespons saat kontrol gagal dalam evaluasinya:
 - Peringatkan — Mengeluarkan peringatan kepada pengguna tetapi memungkinkan tindakan untuk dilanjutkan. Ini berguna untuk validasi non-kritis atau pemeriksaan informasi.
 - Gagal — Mencegah tindakan dari melanjutkan. Ini berguna untuk menegakkan kepatuhan yang ketat atau kebijakan keamanan.
9. Pilih Berikutnya.
10. (Opsional) Untuk filter Hook, lakukan hal berikut:
 - a. Untuk kriteria Pemfilteran, pilih logika untuk menerapkan nama tumpukan dan filter peran tumpukan:
 - Semua nama tumpukan dan peran tumpukan — Hook hanya akan dipanggil ketika semua filter yang ditentukan cocok.

- Setiap nama tumpukan dan peran tumpukan — Hook akan dipanggil jika setidaknya salah satu filter yang ditentukan cocok.
- b. Untuk nama Stack, sertakan atau keculikan tumpukan tertentu dari pemanggilan Hook.
 - Untuk Sertakan, tentukan nama tumpukan yang akan disertakan. Gunakan ini ketika Anda memiliki satu set kecil tumpukan spesifik yang ingin Anda targetkan. Hanya tumpukan yang ditentukan dalam daftar ini yang akan memanggil Hook.
 - Untuk Kecualikan, tentukan nama tumpukan yang akan dikecualikan. Gunakan ini ketika Anda ingin memanggil Hook di sebagian besar tumpukan tetapi mengecualikan beberapa yang spesifik. Semua tumpukan kecuali yang tercantum di sini akan memanggil Hook.
 - c. Untuk peran Stack, sertakan atau keculikan tumpukan tertentu dari pemanggilan Hook berdasarkan peran IAM terkait.
 - Untuk Sertakan, tentukan satu atau beberapa peran IAM ARNs untuk menargetkan tumpukan yang terkait dengan peran ini. Hanya operasi tumpukan yang diprakarsai oleh peran ini yang akan memanggil Hook.
 - Untuk Kecualikan, tentukan satu atau beberapa peran IAM ARNs untuk tumpukan yang ingin Anda keculikan. Hook akan dipanggil pada semua tumpukan kecuali yang diprakarsai oleh peran yang ditentukan.
11. Pilih Berikutnya.
 12. Pada halaman Tinjau dan aktifkan, tinjau pilihan Anda. Untuk membuat perubahan, pilih Edit pada bagian terkait.
 13. Saat Anda siap untuk melanjutkan, pilih Activate Hook.

Aktifkan Hook () berbasis kontrol proaktif AWS CLI

Sebelum melanjutkan, konfirmasikan bahwa Anda telah mengidentifikasi kontrol proaktif yang akan Anda gunakan dengan Hook ini. Untuk informasi selengkapnya, lihat [Katalog AWS Control Tower Kontrol](#).

Untuk mengaktifkan Hook berbasis kontrol proaktif untuk digunakan di akun Anda ()AWS CLI

1. Untuk mulai mengaktifkan Hook, gunakan [activate-type](#) perintah berikut, ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation activate-type --type HOOK \
```

```
--type-name AWS::ControlTower::Hook \  
--publisher-id aws-hooks \  
--type-name-alias MyOrg::Security::ComplianceHook \  
--region us-west-2
```

2. Untuk menyelesaikan pengaktifan Hook, Anda harus mengkonfigurasinya menggunakan file konfigurasi JSON.

Gunakan cat perintah untuk membuat file JSON dengan struktur berikut. Untuk informasi selengkapnya, lihat [Referensi sintaks skema konfigurasi hook](#).

Contoh berikut ini mengonfigurasi Hook yang memanggil sumber daya IAM, Amazon EC2, dan Amazon S3 tertentu selama dan operasi. CREATE UPDATE Ini menerapkan tiga kontrol proaktif (CT.IAM.PR.5,CT.EC2.PR.17,CT.S3.PR.12) untuk memvalidasi sumber daya ini terhadap standar kepatuhan. Hook beroperasi dalam WARN mode, artinya akan menandai sumber daya yang tidak sesuai dengan peringatan tetapi tidak akan memblokir penerapan.

```
$ cat > config.json  
{  
  "CloudFormationConfiguration": {  
    "HookConfiguration": {  
      "HookInvocationStatus": "ENABLED",  
      "TargetOperations": ["RESOURCE"],  
      "FailureMode": "WARN",  
      "Properties": {  
        "ControlsToApply": "CT.IAM.PR.5,CT.EC2.PR.17,CT.S3.PR.12"  
      },  
      "TargetFilters": {  
        "Actions": [  
          "CREATE",  
          "UPDATE"  
        ]  
      }  
    }  
  }  
}
```

- HookInvocationStatus: Setel ENABLED untuk mengaktifkan Hook.
- TargetOperations: Setel ke RESOURCE karena ini adalah satu-satunya nilai yang didukung untuk Hook berbasis kontrol proaktif.
- FailureMode: Setel ke salah satu FAIL atau WARN.

- `ControlsToApply`: Tentukan kontrol kontrol IDs proaktif yang akan digunakan. Untuk informasi selengkapnya, lihat [Katalog AWS Control Tower Kontrol](#).
 - (Opsional)`TargetFilters`: Untuk `Actions`, Anda dapat menentukan `CREATE` atau `UPDATE`, atau keduanya (default), untuk mengontrol kapan Hook dipanggil. Menentukan `CREATE` sendiri membatasi Hook hanya untuk `CREATE` operasi. `TargetFilters` Properti lain tidak berpengaruh.
3. Gunakan [set-type-configuration](#) perintah berikut, bersama dengan file JSON yang Anda buat, untuk menerapkan konfigurasi. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation set-type-configuration \  
  --configuration file://config.json \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-  
Security-ComplianceHook" \  
  --region us-west-2
```

Hapus Hooks berbasis kontrol proaktif di akun Anda

Bila Anda tidak lagi memerlukan Hook berbasis kontrol proaktif yang diaktifkan, gunakan prosedur berikut untuk menghapusnya di akun Anda.

Untuk menonaktifkan sementara Hook alih-alih menghapusnya, lihat [Nonaktifkan dan aktifkan CloudFormation Hooks](#).

Topik

- [Hapus Hook berbasis kontrol proaktif di akun Anda \(konsol\)](#)
- [Hapus Hook berbasis kontrol proaktif di akun Anda \(AWS CLI\)](#)

Hapus Hook berbasis kontrol proaktif di akun Anda (konsol)

Untuk menghapus Hook berbasis kontrol proaktif di akun Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Hook berada.
3. Dari panel navigasi, pilih Hooks.
4. Pada halaman Hooks, temukan Hook berbasis kontrol proaktif yang ingin Anda hapus.

5. Pilih kotak centang di sebelah Hook Anda dan pilih Hapus.
6. Saat diminta konfirmasi, ketikkan nama Hook untuk mengonfirmasi penghapusan Hook yang ditentukan dan kemudian pilih Hapus.

Hapus Hook berbasis kontrol proaktif di akun Anda ()AWS CLI

Note

Sebelum Anda dapat menghapus Hook, Anda harus menonaktifkannya terlebih dahulu. Untuk informasi selengkapnya, lihat [Nonaktifkan dan aktifkan Hook di akun Anda \(AWS CLI\)](#).

Gunakan [deactivate-type](#) perintah berikut untuk menonaktifkan Hook, yang menghapusnya dari akun Anda. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation deactivate-type \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-Security-  
ComplianceHook" \  
  --region us-west-2
```

Kait Pelindung

Untuk menggunakan AWS CloudFormation Guard Hook di akun Anda, Anda harus mengaktifkan Hook untuk akun dan Wilayah tempat Anda ingin menggunakannya. Mengaktifkan Hook membuatnya dapat digunakan dalam operasi tumpukan di akun dan Wilayah tempat Hook diaktifkan.

Saat Anda mengaktifkan Guard Hook, CloudFormation buat entri di registri akun Anda untuk Hook yang diaktifkan sebagai Hook pribadi. Ini memungkinkan Anda untuk mengatur properti konfigurasi apa pun yang disertakan Hook. Properti konfigurasi menentukan bagaimana Hook dikonfigurasi untuk diberikan Akun AWS dan Wilayah.

Topik

- [AWS CLI perintah untuk bekerja dengan Guard Hooks](#)
- [Tulis aturan Guard untuk mengevaluasi sumber daya untuk Guard Hooks](#)
- [Bersiaplah untuk membuat Guard Hook](#)
- [Aktifkan Guard Hook di akun Anda](#)

- [Lihat log untuk Guard Hooks di akun Anda](#)
- [Hapus Guard Hooks di akun Anda](#)

AWS CLI perintah untuk bekerja dengan Guard Hooks

AWS CLI Perintah untuk bekerja dengan Guard Hooks meliputi:

- [activate-type](#) untuk memulai proses aktivasi untuk Guard Hook.
- [set-type-configuration](#) untuk menentukan data konfigurasi untuk Hook di akun Anda.
- [list-types](#) untuk mencantumkan Hooks di akun Anda.
- [describe-type](#) untuk mengembalikan informasi terperinci tentang Hook tertentu atau versi Hook tertentu, termasuk data konfigurasi saat ini.
- [deactivate-type](#) untuk menghapus Hook yang sebelumnya diaktifkan dari akun Anda.

Tulis aturan Guard untuk mengevaluasi sumber daya untuk Guard Hooks

AWS CloudFormation Guard adalah bahasa khusus domain open-source dan tujuan umum (DSL) yang dapat Anda gunakan untuk menulis. `policy-as-code` Topik ini menjelaskan cara menggunakan Guard to author contoh aturan yang dapat dijalankan di Guard Hook untuk mengevaluasi CloudFormation dan AWS Cloud Control API operasi secara otomatis. Ini juga akan fokus pada berbagai jenis input yang tersedia untuk aturan Guard Anda tergantung pada kapan Guard Hook Anda berjalan. Guard Hook dapat dikonfigurasi untuk dijalankan selama jenis operasi berikut:

- Operasi sumber daya
- Operasi tumpukan
- Ubah operasi set

Untuk informasi selengkapnya tentang menulis aturan Penjaga, lihat [AWS CloudFormation Guard Aturan penulisan](#)

Topik

- [Operasi sumber daya Aturan penjaga](#)
- [Aturan Penjaga operasi tumpukan](#)
- [Ubah aturan Penjaga operasi yang ditetapkan](#)

Operasi sumber daya Aturan penjaga

Setiap kali Anda membuat, memperbarui, atau menghapus sumber daya, itu dianggap sebagai operasi sumber daya. Sebagai contoh, jika Anda menjalankan pembaruan CloudFormation tumpukan yang membuat sumber daya baru, Anda telah menyelesaikan operasi sumber daya. Saat Anda membuat, memperbarui, atau menghapus sumber daya menggunakan Cloud Control API, itu juga dianggap sebagai operasi sumber daya. Anda dapat mengkonfigurasi Guard Hook Anda untuk menargetkan RESOURCE dan CLOUD_CONTROL operasi dalam TargetOperations konfigurasi untuk Hook Anda. Ketika Guard Hook Anda mengevaluasi operasi sumber daya, mesin Guard mengevaluasi input sumber daya.

Topik

- [Sintaks masukan sumber daya jaga](#)
- [Contoh masukan operasi sumber daya Guard](#)
- [Aturan penjaga untuk perubahan sumber daya](#)

Sintaks masukan sumber daya jaga

Input sumber daya Guard adalah data yang tersedia untuk aturan Guard Anda untuk dievaluasi.

Berikut ini adalah contoh bentuk input sumber daya:

```
HookContext:
  AWSAccountID: String
  StackId: String
  HookTypeName: String
  HookTypeVersion: String
  InvocationPoint: [CREATE_PRE_PROVISION, UPDATE_PRE_PROVISION, DELETE_PRE_PROVISION]
  TargetName: String
  TargetType: RESOURCE
  TargetLogicalId: String
  ChangeSetId: String
Resources:
  {ResourceLogicalID}:
    ResourceType: {ResourceType}
    ResourceProperties:
      {ResourceProperties}
Previous:
  ResourceLogicalID:
    ResourceType: {ResourceType}
```

ResourceProperties:

```
{PreviousResourceProperties}
```

HookContext**AWSAccountID**

ID yang Akun AWS berisi sumber daya yang sedang dievaluasi.

StackId

ID tumpukan CloudFormation tumpukan yang merupakan bagian dari operasi sumber daya. Ini kosong jika penelepon adalah Cloud Control API.

HookTypeName

Nama Hook yang sedang berjalan.

HookTypeVersion

Versi Hook yang sedang berjalan.

InvocationPoint

Titik yang tepat dalam logika penyediaan tempat Hook berjalan.

Nilai yang valid: (CREATE_PRE_PROVISION| UPDATE_PRE_PROVISION
|DELETE_PRE_PROVISION)

TargetName

Jenis target yang dievaluasi, misalnya,AWS::S3::Bucket.

TargetType

Jenis target yang sedang dievaluasi, misalnyaAWS::S3::Bucket. Untuk sumber daya yang disediakan dengan Cloud Control API, nilai ini akan menjadi. RESOURCE

TargetLogicalId

Sumber TargetLogicalId daya yang sedang dievaluasi. Jika asal Hook adalah CloudFormation, ini akan menjadi ID logis (juga dikenal sebagai nama logis) dari sumber daya. Jika asal Hook adalah Cloud Control API, ini akan menjadi nilai yang dibangun.

ChangeSetId

Perubahan set ID yang dieksekusi menyebabkan pemanggilan Hook. Nilai ini kosong jika perubahan sumber daya dimulai oleh Cloud Control API, atau `create-stackupdate-stack`, atau `delete-stack` operasi.

Resources

ResourceLogicalID

Ketika operasi dimulai oleh CloudFormation, `ResourceLogicalID` adalah ID logis dari sumber daya dalam CloudFormation template.

Ketika operasi dimulai oleh Cloud Control API, `ResourceLogicalID` ini adalah kombinasi dari jenis sumber daya, nama, ID operasi, dan ID permintaan.

ResourceType

Jenis nama sumber daya (contoh: `AWS::S3::Bucket`).

ResourceProperties

Properti yang diusulkan dari sumber daya yang sedang dimodifikasi. Saat Guard Hook berjalan melawan perubahan CloudFormation sumber daya, fungsi, parameter, dan transformasi apa pun akan diselesaikan sepenuhnya. Jika sumber daya dihapus, nilai ini akan kosong.

Previous

ResourceLogicalID

Ketika operasi dimulai oleh CloudFormation, `ResourceLogicalID` adalah ID logis dari sumber daya dalam CloudFormation template.

Ketika operasi dimulai oleh Cloud Control API, `ResourceLogicalID` ini adalah kombinasi dari jenis sumber daya, nama, ID operasi, dan ID permintaan.

ResourceType

Jenis nama sumber daya (contoh: `AWS::S3::Bucket`).

ResourceProperties

Properti saat ini terkait dengan sumber daya yang sedang dimodifikasi. Jika sumber daya dihapus, nilai ini akan kosong.

Contoh masukan operasi sumber daya Guard

Contoh masukan berikut menunjukkan Guard Hook yang akan menerima definisi

`AWS::S3::Bucket` sumber daya untuk diperbarui. Ini adalah data yang tersedia untuk Guard untuk evaluasi.

```
HookContext:
  AwsAccountId: "123456789012"
  StackId: "arn:aws:cloudformation:us-west-2:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000"
  HookTypeName: org::s3policy::hook
  HookTypeVersion: "00001"
  InvocationPoint: UPDATE_PRE_PROVISION
  TargetName: AWS::S3::Bucket
  TargetType: RESOURCE
  TargetLogicalId: MyS3Bucket
  ChangeSetId: ""
Resources:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      ObjectLockEnabled: true
Previous:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      ObjectLockEnabled: false
```

Untuk melihat semua properti yang tersedia untuk jenis sumber daya, lihat [AWS::S3::Bucket](#).

Aturan penjaga untuk perubahan sumber daya

Ketika Guard Hook mengevaluasi perubahan sumber daya, itu dimulai dengan mengunduh semua aturan yang dikonfigurasi dengan Hook. Aturan-aturan ini kemudian dievaluasi terhadap input sumber daya. Hook akan gagal jika ada aturan yang gagal dalam evaluasi mereka. Jika tidak ada kegagalan, Hook akan lewat.

Contoh berikut adalah aturan Guard yang mengevaluasi apakah `ObjectLockEnabled` properti adalah `true` untuk jenis `AWS::S3::Bucket` sumber daya apa pun.

```
let s3_buckets_default_lock_enabled = Resources.*[ Type == 'AWS::S3::Bucket']
```

```
rule S3_BUCKET_DEFAULT_LOCK_ENABLED when %s3_buckets_default_lock_enabled !empty {
  %s3_buckets_default_lock_enabled.Properties.ObjectLockEnabled exists
  %s3_buckets_default_lock_enabled.Properties.ObjectLockEnabled == true
  <<
    Violation: S3 Bucket ObjectLockEnabled must be set to true.
    Fix: Set the S3 property ObjectLockEnabled parameter to true.
  >>
}
```

Ketika aturan ini berjalan terhadap input berikut, itu akan gagal karena `ObjectLockEnabled` properti tidak disetel ke `true`.

```
Resources:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      ObjectLockEnabled: false
```

Ketika aturan ini berjalan terhadap input berikut, itu akan berlalu karena `ObjectLockEnabled` diatur ke `true`.

```
Resources:
  MyS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: amzn-s3-demo-bucket
      ObjectLockEnabled: true
```

Ketika Hook gagal, aturan yang gagal akan disebarkan kembali ke CloudFormation atau Cloud Control API. Jika bucket logging telah dikonfigurasi untuk Guard Hook, umpan balik aturan tambahan akan diberikan di sana. Umpan balik tambahan ini mencakup `Violation` dan `Fix` informasi.

Aturan Penjaga operasi tumpukan

Saat CloudFormation tumpukan dibuat, diperbarui, atau dihapus, Anda dapat mengonfigurasi Guard Hook untuk memulai dengan mengevaluasi template baru dan berpotensi memblokir operasi tumpukan agar tidak dilanjutkan. Anda dapat mengonfigurasi Guard Hook Anda untuk menargetkan `STACK` operasi dalam `TargetOperations` konfigurasi untuk Hook Anda.

Topik

- [Sintaks masukan tumpukan penjaga](#)
- [Contoh masukan operasi tumpukan Guard](#)
- [Aturan penjaga untuk perubahan tumpukan](#)

Sintaks masukan tumpukan penjaga

Input untuk operasi tumpukan Guard menyediakan seluruh CloudFormation template untuk dievaluasi aturan Guard Anda.

Berikut ini adalah contoh bentuk input stack:

```
HookContext:
  AWSAccountID: String
  StackId: String
  HookTypeName: String
  HookTypeVersion: String
  InvocationPoint: [CREATE_PRE_PROVISION, UPDATE_PRE_PROVISION, DELETE_PRE_PROVISION]
  TargetName: String
  TargetType: STACK
  ChangeSetId: String
  {Proposed CloudFormation Template}
Previous:
  {CloudFormation Template}
```

HookContext

AWSAccountID

ID yang Akun AWS berisi sumber daya.

StackId

ID tumpukan CloudFormation tumpukan yang merupakan bagian dari operasi tumpukan.

HookTypeName

Nama Hook yang sedang berjalan.

HookTypeVersion

Versi Hook yang sedang berjalan.

InvocationPoint

Titik yang tepat dalam logika penyediaan tempat Hook berjalan.

Nilai yang valid: (CREATE_PRE_PROVISION| UPDATE_PRE_PROVISION
|DELETE_PRE_PROVISION)

TargetName

Nama tumpukan yang sedang dievaluasi.

TargetType

Nilai ini akan STACK saat dijalankan sebagai Hook tingkat tumpukan.

ChangeSetId

Perubahan set ID yang dieksekusi menyebabkan pemanggilan Hook. Nilai ini kosong jika operasi tumpukan dimulai oleh `create-stack`, `update-stack`, atau `delete-stack` operasi.

Proposed CloudFormation Template

Nilai CloudFormation template lengkap yang diteruskan ke CloudFormation `create-stack` atau `update-stack` operasi. Ini termasuk hal-hal seperti `Resources`, `Outputs`, dan `Properties`. Ini bisa berupa string JSON atau YAML tergantung pada apa yang disediakan. CloudFormation

Dalam `delete-stack` operasi, nilai ini akan kosong.

Previous

CloudFormation Template terakhir berhasil digunakan. Nilai ini kosong jika tumpukan sedang dibuat atau dihapus.

Dalam `delete-stack` operasi, nilai ini akan kosong.

Note

Template yang disediakan adalah apa yang diteruskan ke `create` atau `update` tumpukan operasi. Saat menghapus tumpukan, tidak ada nilai templat yang disediakan.

Contoh masukan operasi tumpukan Guard

Contoh masukan berikut menunjukkan Guard Hook yang akan menerima template lengkap dan template yang sebelumnya digunakan. Template dalam contoh ini menggunakan format JSON.

```
HookContext:
  AwsAccountId: 123456789012
  StackId: "arn:aws:cloudformation:us-west-2:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000"
  HookTypeName: org::templatechecker::hook
  HookTypeVersion: "00001"
  InvocationPoint: UPDATE_PRE_PROVISION
  TargetName: MyStack
  TargetType: CHANGE_SET
  TargetLogicalId: arn:aws:cloudformation:us-west-2:123456789012:changeSet/
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000
  ChangeSetId: arn:aws:cloudformation:us-west-2:123456789012:changeSet/
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000
Resources: {
  "S3Bucket": {
    "Type": "AWS::S3::Bucket",
    "Properties": {
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {"ServerSideEncryptionByDefault":
            {"SSEAlgorithm": "aws:kms",
             "KMSMasterKeyID": "KMS-KEY-ARN" }},
          {"BucketKeyEnabled": true }
        ]
      }
    }
  }
}
Previous: {
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "S3Bucket": {
      "Type": "AWS::S3::Bucket",
      "Properties": {}
    }
  }
}
```

Aturan penjaga untuk perubahan tumpukan

Ketika Guard Hook mengevaluasi perubahan tumpukan, itu dimulai dengan mengunduh semua aturan yang dikonfigurasi dengan Hook. Aturan-aturan ini kemudian dievaluasi terhadap input sumber daya. Hook akan gagal jika ada aturan yang gagal dalam evaluasi mereka. Jika tidak ada kegagalan, Hook akan lewat.

Contoh berikut adalah aturan Guard yang mengevaluasi jika ada jenis `AWS::S3::Bucket` sumber daya yang berisi properti `BucketEncryption`, dengan `SSEAlgorithm` set ke salah satu `aws:kms` atau `AES256`.

```
let s3_buckets_s3_default_encryption = Resources.*[ Type == 'AWS::S3::Bucket']

rule S3_DEFAULT_ENCRYPTION_KMS when %s3_buckets_s3_default_encryption !empty {
  %s3_buckets_s3_default_encryption.Properties.BucketEncryption exists

  %s3_buckets_s3_default_encryption.Properties.BucketEncryption.ServerSideEncryptionConfiguration
  in ["aws:kms","AES256"]
  <<
    Violation: S3 Bucket default encryption must be set.
    Fix: Set the S3 Bucket property
    BucketEncryption.ServerSideEncryptionConfiguration.ServerSideEncryptionByDefault.SSEAlgorithm
    to either "aws:kms" or "AES256"
  >>
}
```

Ketika aturan berjalan terhadap template berikut, itu akan `fail`.

```
AWSTemplateFormatVersion: 2010-09-09
Description: S3 bucket without default encryption
Resources:
  EncryptedS3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
```

Ketika aturan berjalan terhadap template berikut, itu akan `pass`.

```
AWSTemplateFormatVersion: 2010-09-09
Description: S3 bucket with default encryption using SSE-KMS with an S3 Bucket Key
Resources:
```

```

EncryptedS3Bucket:
  Type: 'AWS::S3::Bucket'
  Properties:
    BucketName: !Sub 'encryptedbucket-${AWS::Region}-${AWS::AccountId}'
    BucketEncryption:
      ServerSideEncryptionConfiguration:
        - ServerSideEncryptionByDefault:
            SSEAlgorithm: 'aws:kms'
            KMSMasterKeyID: KMS-KEY-ARN
            BucketKeyEnabled: true

```

Ubah aturan Penjaga operasi yang ditetapkan

Saat set CloudFormation perubahan dibuat, Anda dapat mengonfigurasi Guard Hook untuk mengevaluasi template dan perubahan yang diusulkan dalam set perubahan untuk memblokir eksekusi set perubahan.

Topik

- [Perubahan penjaga mengatur sintaks masukan](#)
- [Contoh Guard mengubah set masukan operasi](#)
- [Aturan penjaga untuk operasi set perubahan](#)

Perubahan penjaga mengatur sintaks masukan

Input set perubahan Guard adalah data yang tersedia untuk aturan Guard Anda untuk dievaluasi.

Berikut ini adalah contoh bentuk dari input set perubahan:

```

HookContext:
  AWSAccountID: String
  StackId: String
  HookTypeName: String
  HookTypeVersion: String
  InvocationPoint: [CREATE_PRE_PROVISION, UPDATE_PRE_PROVISION, DELETE_PRE_PROVISION]
  TargetName: CHANGE_SET
  TargetType: CHANGE_SET
  TargetLogicalId: ChangeSet ID
  ChangeSetId: String
  Proposed CloudFormation Template
  Previous:

```

```
{CloudFormation Template}
Changes: [{ResourceChange}]
```

Sintaks ResourceChange model adalah:

```
logicalResourceId: String
resourceType: String
tindakan: CREATE, UPDATE, DELETE
LineNumber: Number
sebelumKonteks: JSON String
AfterContext: JSON String
```

HookContext

AWSAccountID

ID yang Akun AWS berisi sumber daya.

StackId

ID tumpukan CloudFormation tumpukan yang merupakan bagian dari operasi tumpukan.

HookTypeName

Nama Hook yang sedang berjalan.

HookTypeVersion

Versi Hook yang sedang berjalan.

InvocationPoint

Titik yang tepat dalam logika penyediaan tempat Hook berjalan.

Nilai yang valid: (CREATE_PRE_PROVISION| UPDATE_PRE_PROVISION
|DELETE_PRE_PROVISION)

TargetName

Nama tumpukan yang sedang dievaluasi.

TargetType

Nilai ini akan CHANGE_SET ketika berjalan sebagai perubahan set-level Hook.

TargetLogicalId

Nilai ini akan menjadi ARN dari set perubahan.

ChangeSetId

Perubahan set ID yang dieksekusi menyebabkan pemanggilan Hook. Nilai ini kosong jika operasi tumpukan dimulai oleh `create-stack`, `update-stack`, atau `delete-stack` operasi.

Proposed CloudFormation Template

CloudFormation Template lengkap yang disediakan untuk `create-change-set` operasi. Ini bisa berupa string JSON atau YAMAL tergantung pada apa yang disediakan. CloudFormation

Previous

CloudFormation Template terakhir berhasil digunakan. Nilai ini kosong jika tumpukan sedang dibuat atau dihapus.

Changes

`ChangesModelnya`. Ini mencantumkan perubahan sumber daya.

Perubahan

logicalResourceId

Nama sumber daya logis dari sumber daya yang diubah.

resourceType

Jenis sumber daya yang akan diubah.

tindakan

Jenis operasi yang dilakukan pada sumber daya.

Nilai yang valid: (CREATE| UPDATE |DELETE)

LineNumber

Nomor baris dalam template yang terkait dengan perubahan.

sebelumKonteks

Sebuah string JSON properti sumber daya sebelum perubahan:

```
{"properties": {"property1": "value"}}
```

AfterContext

Sebuah string JSON properti sumber daya setelah perubahan:

```
{"properties": {"property1": "new value"}}
```

Contoh Guard mengubah set masukan operasi

Contoh masukan berikut menunjukkan Guard Hook yang akan menerima template lengkap, template yang sebelumnya digunakan, dan daftar perubahan sumber daya. Template dalam contoh ini menggunakan format JSON.

```
HookContext:
  AwsAccountId: "00000000"
  StackId: MyStack
  HookTypeName: org::templatechecker::hook
  HookTypeVersion: "00001"
  InvocationPoint: UPDATE_PRE_PROVISION
  TargetName: my-example-stack
  TargetType: STACK
  TargetLogicalId: arn...:changeSet/change-set
  ChangeSetId: ""
Resources: {
  "S3Bucket": {
    "Type": "AWS::S3::Bucket",
    "Properties": {
      "BucketName": "amzn-s3-demo-bucket",
      "VersioningConfiguration": {
        "Status": "Enabled"
      }
    }
  }
}
Previous: {
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "S3Bucket": {
      "Type": "AWS::S3::Bucket",
      "Properties": {
        "BucketName": "amzn-s3-demo-bucket",
```

```

        "VersioningConfiguration":{
            "Status": "Suspended"
        }
    }
}
}
}
Changes: [
    {
        "logicalResourceId": "S3Bucket",
        "resourceType": "AWS::S3::Bucket",
        "action": "UPDATE",
        "lineNumber": 5,
        "beforeContext": "{\"Properties\":{\"VersioningConfiguration\":{\"Status\":
\"Suspended\"}}}",
        "afterContext": "{\"Properties\":{\"VersioningConfiguration\":{\"Status\": \"Enabled
\"}}}"
    }
]

```

Aturan penjaga untuk operasi set perubahan

Contoh berikut adalah aturan Penjaga yang mengevaluasi perubahan pada bucket Amazon S3, dan memastikan VersionConfiguration bahwa tidak dinonaktifkan.

```

let s3_buckets_changing = Changes[resourceType == 'AWS::S3::Bucket']

rule S3_VERSIONING_STAY_ENABLED when %s3_buckets_changing !empty {
    let afterContext = json_parse(%s3_buckets_changing.afterContext)
    when %afterContext.Properties.VersioningConfiguration.Status !empty {
        %afterContext.Properties.VersioningConfiguration.Status == 'Enabled'
    }
}

```

Bersiaplah untuk membuat Guard Hook

Sebelum Anda membuat Guard Hook, Anda harus menyelesaikan prasyarat berikut:

- Anda pasti sudah membuat aturan Penjaga. Untuk informasi selengkapnya, lihat [Tulis aturan Guard untuk Hooks](#).

- Pengguna atau peran yang membuat Hook harus memiliki izin yang cukup untuk mengaktifkan Hooks. Untuk informasi selengkapnya, lihat [Berikan izin IAM untuk Hooks CloudFormation](#).
- Untuk menggunakan AWS CLI atau SDK untuk membuat Guard Hook, Anda harus secara manual membuat peran eksekusi dengan izin IAM dan kebijakan kepercayaan CloudFormation untuk memungkinkan memanggil Guard Hook.

Buat peran eksekusi untuk Guard Hook

Hook menggunakan peran eksekusi untuk izin yang diperlukan untuk memanggil Hook itu di Akun AWS.

Peran ini dapat dibuat secara otomatis jika Anda membuat Guard Hook dari Konsol Manajemen AWS; jika tidak, Anda harus membuat peran ini sendiri.

Bagian berikut menunjukkan cara mengatur izin untuk membuat Guard Hook Anda.

Izin yang diperlukan

Ikuti panduan di [Membuat peran menggunakan kebijakan kepercayaan khusus](#) di Panduan Pengguna IAM untuk membuat peran dengan kebijakan kepercayaan khusus.

Kemudian, selesaikan langkah-langkah berikut untuk mengatur izin Anda:

1. Lampirkan kebijakan hak istimewa minimum berikut ke peran IAM yang ingin Anda gunakan untuk membuat Guard Hook.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3::my-guard-output-bucket/*",
        "arn:aws:s3::my-guard-rules-bucket"
      ]
    }
  ]
}
```

```
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::my-guard-output-bucket/*"
    ]
  }
]
```

2. Berikan izin Hook Anda untuk mengambil peran dengan menambahkan kebijakan kepercayaan ke peran tersebut. Berikut ini menunjukkan contoh kebijakan kepercayaan yang dapat Anda gunakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "hooks.cloudformation.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Aktifkan Guard Hook di akun Anda

Topik berikut menunjukkan kepada Anda cara mengaktifkan Guard Hook di akun Anda, yang membuatnya dapat digunakan di akun dan Wilayah tempat diaktifkan.

Topik

- [Aktifkan Guard Hook \(konsol\)](#)
- [Aktifkan Guard Hook \(AWS CLI\)](#)
- [Sumber daya terkait](#)

Aktifkan Guard Hook (konsol)

Untuk mengaktifkan Guard Hook untuk digunakan di akun Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Anda ingin membuat Hook.
3. Di panel navigasi di sebelah kiri, pilih Hooks.
4. Pada halaman Hooks, pilih Create a Hook, lalu pilih With Guard.
5. Jika Anda belum membuat aturan Guard, buat aturan Guard Anda, simpan di Amazon S3, lalu kembali ke prosedur ini. Lihat contoh aturan [Tulis aturan Guard untuk mengevaluasi sumber daya untuk Guard Hooks](#) untuk memulai.

Jika Anda telah membuat aturan Guard dan menyimpannya di S3, lanjutkan ke langkah berikutnya.

Note

Objek yang disimpan di S3 harus memiliki salah satu ekstensi file berikut: `.guard`, `.zip`, atau `.tar.gz`.

6. Untuk sumber Guard Hook, Simpan aturan Guard Anda di S3, lakukan hal berikut:
 - Untuk URI S3, tentukan jalur S3 ke file aturan Anda atau gunakan tombol Browse S3 untuk membuka kotak dialog untuk menelusuri dan memilih objek S3.
 - (Opsional) Untuk versi Object, jika bucket S3 Anda mengaktifkan versi, Anda dapat memilih versi tertentu dari objek S3.


Guard Hook mengunduh aturan Anda dari S3 setiap kali Hook dipanggil. Untuk mencegah perubahan atau penghapusan yang tidak disengaja, sebaiknya gunakan versi saat mengonfigurasi Guard Hook Anda.

7. (Opsional) Untuk bucket S3 untuk laporan keluaran Guard, tentukan bucket S3 untuk menyimpan laporan keluaran Guard. Laporan ini berisi hasil validasi aturan Guard Anda.

Untuk mengonfigurasi tujuan laporan keluaran, pilih salah satu opsi berikut:

- Pilih kotak centang Gunakan ember yang sama aturan Penjaga saya disimpan di kotak centang untuk menggunakan bucket yang sama tempat aturan Guard Anda berada.
 - Pilih nama bucket S3 yang berbeda untuk menyimpan laporan keluaran Guard.
8. (Opsional) Perluas parameter input aturan Guard, lalu berikan informasi berikut di bawah Simpan parameter input aturan Guard Anda di S3:
 - Untuk URI S3, tentukan jalur S3 ke file parameter atau gunakan tombol Browse S3 untuk membuka kotak dialog untuk menelusuri dan memilih objek S3.
 - (Opsional) Untuk versi Object, jika bucket S3 Anda mengaktifkan versi, Anda dapat memilih versi tertentu dari objek S3.
 9. Pilih Berikutnya.
 10. Untuk nama Hook, pilih salah satu opsi berikut:
 - Berikan nama deskriptif singkat yang akan ditambahkan setelahnya `Private::Guard::`. Misalnya, jika Anda masuk `MyTestHook`, nama Hook lengkap menjadi `Private::Guard::MyTestHook`.
 - Berikan nama Hook lengkap (juga disebut alias) menggunakan format ini:
`Provider::ServiceName::HookName`
 11. Untuk target Hook, pilih apa yang akan dievaluasi:
 - Stacks - Mengevaluasi template tumpukan saat pengguna membuat, memperbarui, atau menghapus tumpukan.
 - Sumber Daya - Mengevaluasi perubahan sumber daya individu saat pengguna memperbarui tumpukan.
 - Ubah set - Mengevaluasi pembaruan yang direncanakan saat pengguna membuat set perubahan.
 - Cloud Control API - Mengevaluasi membuat, memperbarui, atau menghapus operasi yang diprakarsai oleh [Cloud Control](#) API.
 12. Untuk Tindakan, pilih tindakan mana (buat, perbarui, hapus) yang akan memanggil Hook Anda.
 13. Untuk mode Hook, pilih bagaimana Hook merespons ketika aturan gagal evaluasi mereka:

- Peringatkan — Mengeluarkan peringatan kepada pengguna tetapi memungkinkan tindakan untuk dilanjutkan. Ini berguna untuk validasi non-kritis atau pemeriksaan informasi.
 - Gagal — Mencegah tindakan dari melanjutkan. Ini berguna untuk menegakkan kepatuhan yang ketat atau kebijakan keamanan.
14. Untuk peran Eksekusi, pilih peran IAM yang diasumsikan Hook untuk mengambil aturan Guard Anda dari S3 dan secara opsional menulis laporan keluaran Guard terperinci kembali. Anda dapat mengizinkan CloudFormation untuk secara otomatis membuat peran eksekusi untuk Anda atau Anda dapat menentukan peran yang telah Anda buat.
 15. Pilih Berikutnya.
 16. (Opsional) Untuk filter Hook, lakukan hal berikut:
 - a. Untuk filter Sumber Daya, tentukan jenis sumber daya mana yang dapat memanggil Hook. Ini memastikan bahwa Hook hanya dipanggil untuk sumber daya yang relevan.
 - b. Untuk kriteria Pemfilteran, pilih logika untuk menerapkan nama tumpukan dan filter peran tumpukan:
 - Semua nama tumpukan dan peran tumpukan — Hook hanya akan dipanggil ketika semua filter yang ditentukan cocok.
 - Setiap nama tumpukan dan peran tumpukan — Hook akan dipanggil jika setidaknya salah satu filter yang ditentukan cocok.
 - c. Untuk nama Stack, sertakan atau keculikan tumpukan tertentu dari pemanggilan Hook.
 - Untuk Sertakan, tentukan nama tumpukan yang akan disertakan. Gunakan ini ketika Anda memiliki satu set kecil tumpukan spesifik yang ingin Anda targetkan. Hanya tumpukan yang ditentukan dalam daftar ini yang akan memanggil Hook.
 - Untuk Kecualikan, tentukan nama tumpukan yang akan dikecualikan. Gunakan ini ketika Anda ingin memanggil Hook di sebagian besar tumpukan tetapi mengecualikan beberapa yang spesifik. Semua tumpukan kecuali yang tercantum di sini akan memanggil Hook.

 Note

Untuk operasi Cloud Control API, semua nama Stack dan filter peran Stack diabaikan.

- d. Untuk peran Stack, sertakan atau kecualikan tumpukan tertentu dari pemanggilan Hook berdasarkan peran IAM terkait.
 - Untuk Sertakan, tentukan satu atau beberapa peran IAM ARNs untuk menargetkan tumpukan yang terkait dengan peran ini. Hanya operasi tumpukan yang diprakarsai oleh peran ini yang akan memanggil Hook.
 - Untuk Kecualikan, tentukan satu atau beberapa peran IAM ARNs untuk tumpukan yang ingin Anda kecualikan. Hook akan dipanggil pada semua tumpukan kecuali yang diprakarsai oleh peran yang ditentukan.

17. Pilih Berikutnya.

18. Pada halaman Tinjau dan aktifkan, tinjau pilihan Anda. Untuk membuat perubahan, pilih Edit pada bagian terkait.

19. Saat Anda siap untuk melanjutkan, pilih Activate Hook.

Aktifkan Guard Hook (AWS CLI)

Sebelum melanjutkan, konfirmasikan bahwa Anda telah membuat aturan Guard dan peran eksekusi yang akan Anda gunakan dengan Hook ini. Untuk informasi selengkapnya, lihat [Tulis aturan Guard untuk mengevaluasi sumber daya untuk Guard Hooks](#) dan [Buat peran eksekusi untuk Guard Hook](#).

Untuk mengaktifkan Guard Hook untuk digunakan di akun Anda (AWS CLI)

1. Untuk mulai mengaktifkan Hook, gunakan [activate-type](#) perintah berikut, ganti placeholder dengan nilai spesifik Anda. Perintah ini mengotorisasi Hook untuk menggunakan peran eksekusi tertentu dari Anda Akun AWS.

```
aws cloudformation activate-type --type HOOK \  
  --type-name AWS::Hooks::GuardHook \  
  --publisher-id aws-hooks \  
  --type-name-alias Private::Guard::MyTestHook \  
  --execution-role-arn arn:aws:iam::123456789012:role/my-execution-role \  
  --region us-west-2
```

2. Untuk menyelesaikan pengaktifan Hook, Anda harus mengkonfigurasinya menggunakan file konfigurasi JSON.

Gunakan cat perintah untuk membuat file JSON dengan struktur berikut. Untuk informasi selengkapnya, lihat [Referensi sintaks skema konfigurasi hook](#).

```
$ cat > config.json
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE",
        "CHANGE_SET"
      ],
      "FailureMode": "WARN",
      "Properties": {
        "ruleLocation": "s3://amzn-s3-demo-bucket/MyGuardRules.guard",
        "logBucket": "amzn-s3-demo-logging-bucket"
      },
      "TargetFilters": {
        "Actions": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ]
      }
    }
  }
}
```

- `HookInvocationStatus`: Setel `ENABLED` untuk mengaktifkan Hook.
 - `TargetOperations`: Tentukan operasi yang akan dievaluasi oleh Hook.
 - `FailureMode`: Setel ke salah satu `FAIL` atau `WARN`.
 - `ruleLocation`: Ganti dengan URI S3 tempat aturan Anda disimpan. Objek yang disimpan di S3 harus memiliki salah satu ekstensi file berikut: `.guard`, `.zip`, dan `.tar.gz`
 - `logBucket`: (Opsional) Tentukan nama bucket S3 untuk laporan Guard JSON.
 - `TargetFilters`: Tentukan jenis tindakan yang akan memanggil Hook.
3. Gunakan [set-type-configuration](#) perintah berikut, bersama dengan file JSON yang Anda buat, untuk menerapkan konfigurasi. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation set-type-configuration \
  --configuration file://config.json \
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \
```

```
--region us-west-2
```

Sumber daya terkait

Kami menyediakan contoh template yang dapat Anda gunakan untuk memahami cara mendeklarasikan Guard Hook dalam template CloudFormation tumpukan. Untuk informasi selengkapnya, lihat [AWS::CloudFormation::GuardHook](#) di AWS CloudFormation Panduan Pengguna.

Lihat log untuk Guard Hooks di akun Anda

Saat mengaktifkan Guard Hook, Anda dapat menentukan bucket Amazon S3 sebagai tujuan laporan keluaran Hook. Setelah diaktifkan, Hook secara otomatis menyimpan hasil validasi aturan Guard Anda di bucket yang ditentukan. Anda kemudian dapat melihat hasil ini di konsol Amazon S3.

Lihat log Guard Hook di konsol Amazon S3

Untuk melihat file log keluaran Guard Hook

1. Masuk ke <https://console.aws.amazon.com/s3/>
2. Pada bilah navigasi di bagian atas layar, pilih Anda Wilayah AWS.
3. Pilih Ember.
4. Pilih bucket yang Anda pilih untuk laporan keluaran Guard.
5. Pilih file log laporan keluaran validasi yang diinginkan.
6. Pilih apakah Anda ingin Mengunduh file atau Buka untuk melihat.

Hapus Guard Hooks di akun Anda

Bila Anda tidak lagi membutuhkan Guard Hook yang diaktifkan, gunakan prosedur berikut untuk menghapusnya di akun Anda.

Untuk menonaktifkan sementara Hook alih-alih menghapusnya, lihat [Nonaktifkan dan aktifkan CloudFormation Hooks](#).

Topik

- [Hapus Guard Hook di akun Anda \(konsol\)](#)
- [Menghapus Guard Hook di akun Anda \(AWS CLI\)](#)

Hapus Guard Hook di akun Anda (konsol)

Untuk menghapus Guard Hook di akun Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Hook berada.
3. Dari panel navigasi, pilih Hooks.
4. Pada halaman Hooks, temukan Guard Hook yang ingin Anda hapus.
5. Pilih kotak centang di sebelah Hook Anda dan pilih Hapus.
6. Saat diminta konfirmasi, ketikkan nama Hook untuk mengonfirmasi penghapusan Hook yang ditentukan dan kemudian pilih Hapus.

Menghapus Guard Hook di akun Anda (AWS CLI)

Note

Sebelum Anda dapat menghapus Hook, Anda harus menonaktifkannya terlebih dahulu. Untuk informasi selengkapnya, lihat [Nonaktifkan dan aktifkan Hook di akun Anda \(AWS CLI\)](#).

Gunakan [deactivate-type](#) perintah berikut untuk menonaktifkan Hook, yang menghapusnya dari akun Anda. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation deactivate-type \  
--type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \  
--region us-west-2
```

Kait Lambda

Untuk menggunakan AWS Lambda Hook di akun Anda, Anda harus terlebih dahulu mengaktifkan Hook untuk akun dan Wilayah tempat Anda ingin menggunakannya. Mengaktifkan Hook membuatnya dapat digunakan dalam operasi tumpukan di akun dan Wilayah tempat Hook diaktifkan.

Saat Anda mengaktifkan Lambda Hook, CloudFormation buat entri di registri akun Anda untuk Hook yang diaktifkan sebagai Hook pribadi. Ini memungkinkan Anda untuk mengatur properti konfigurasi

apa pun yang disertakan Hook. Properti konfigurasi menentukan bagaimana Hook dikonfigurasi untuk diberikan Akun AWS dan Wilayah.

Topik

- [AWS CLI perintah untuk bekerja dengan Lambda Hooks](#)
- [Buat fungsi Lambda untuk mengevaluasi sumber daya untuk Lambda Hooks](#)
- [Bersiaplah untuk membuat Lambda Hook](#)
- [Aktifkan Lambda Hook di akun Anda](#)
- [Lihat log untuk Lambda Hooks di akun Anda](#)
- [Hapus Lambda Hooks di akun Anda](#)

AWS CLI perintah untuk bekerja dengan Lambda Hooks

AWS CLI Perintah untuk bekerja dengan Lambda Hooks meliputi:

- [activate-type](#) untuk memulai proses aktivasi untuk Lambda Hook.
- [set-type-configuration](#) untuk menentukan data konfigurasi untuk Hook di akun Anda.
- [list-types](#) untuk mencantumkan Hooks di akun Anda.
- [describe-type](#) untuk mengembalikan informasi terperinci tentang Hook tertentu atau versi Hook tertentu, termasuk data konfigurasi saat ini.
- [deactivate-type](#) untuk menghapus Hook yang sebelumnya diaktifkan dari akun Anda.

Buat fungsi Lambda untuk mengevaluasi sumber daya untuk Lambda Hooks

CloudFormation Lambda Hooks memungkinkan Anda untuk mengevaluasi CloudFormation dan AWS Cloud Control API operasi terhadap kode kustom Anda sendiri. Hook Anda dapat memblokir operasi agar tidak berjalan, atau mengeluarkan peringatan kepada penelepon dan memungkinkan operasi dilanjutkan. Saat Anda membuat Lambda Hook, Anda dapat mengonfigurasinya untuk mencegah dan mengevaluasi operasi berikut: CloudFormation

- Operasi sumber daya
- Operasi tumpukan
- Ubah operasi set

Topik

- [Mengembangkan Lambda Hook](#)
- [Mengevaluasi operasi sumber daya dengan Lambda Hooks](#)
- [Mengevaluasi operasi tumpukan dengan Lambda Hooks](#)
- [Mengevaluasi operasi set perubahan dengan Lambda Hooks](#)

Mengembangkan Lambda Hook

Saat Hooks memanggil Lambda Anda, Lambda akan menunggu hingga 30 detik hingga Lambda mengevaluasi input. Lambda akan mengembalikan respons JSON yang menunjukkan apakah Hook berhasil atau gagal.

Topik

- [Minta masukan](#)
- [Masukan respons](#)
- [Contoh](#)

Minta masukan

Input yang diteruskan ke fungsi Lambda Anda bergantung pada operasi target Hook (contoh: tumpukan, sumber daya, atau set perubahan).

Masukan respons

Untuk berkomunikasi dengan Hooks jika permintaan Anda berhasil atau gagal, fungsi Lambda Anda perlu mengembalikan respons JSON.

Berikut ini adalah contoh bentuk respons yang diharapkan Hooks:

```
{
  "HookStatus": "SUCCESS" or "FAILED" or "IN_PROGRESS",
  "errorCode": "NonCompliant" or "InternalFailure"
  "pesan": String,
  "clientRequestToken": String,
  "CallbackContext": None,
  "callbackDelaySeconds": Integer,
  "anotasi": [
```

```
{
  "annotationName": String,
  "status": "PASSED" or "FAILED" or "SKIPPED",
  "statusMessage": String,
  "remediationMessage": String,
  "remediationLink": String,
  "severityLevel": "INFORMATIONAL" or "LOW" or "MEDIUM" or "HIGH" or "CRITICAL"
}
]
```

HookStatus

Status Hook. Bidang ini harus diisi.

Nilai yang valid: (SUCCESS| FAILED |IN_PROGRESS)

Note

Hook dapat kembali IN_PROGRESS 3 kali. Jika tidak ada hasil yang dikembalikan, Hook akan gagal. Untuk Lambda Hook, ini berarti fungsi Lambda Anda dapat dipanggil hingga 3 kali.

errorCode

Menunjukkan apakah operasi dievaluasi dan ditentukan tidak valid, atau jika kesalahan terjadi dalam Hook, mencegah evaluasi. Bidang ini diperlukan jika Hook gagal.

Nilai yang valid: (NonCompliant|InternalFailure)

pesan

Pesan kepada penelepon yang menyatakan mengapa Hook berhasil atau gagal.

Note

Saat mengevaluasi CloudFormation operasi, bidang ini dipotong menjadi 4096 karakter. Saat mengevaluasi operasi Cloud Control API, bidang ini dipotong menjadi 1024 karakter.

clientRequestToken

Token permintaan yang disediakan sebagai masukan untuk permintaan Hook. Bidang ini harus diisi.

CallbackContext

Jika Anda menunjukkan bahwa `hookStatus` is, `IN_PROGRESS` Anda meneruskan konteks tambahan yang disediakan sebagai input saat fungsi Lambda dipanggil kembali.

callbackDelaySeconds

Berapa lama Hooks harus menunggu untuk memanggil Hook ini lagi.

anotasi

Sebuah array objek anotasi yang memberikan rincian lebih lanjut dan panduan remediasi.

Nama anotasi

Pengidentifikasi untuk anotasi.

status

Status pemanggilan Hook. Ini membantu ketika anotasi mewakili logika dengan evaluasi lulus/gagal yang mirip dengan aturan Guard.

Nilai yang valid: (PASSED| FAILED |SKIPPED)

StatusMessage

Penjelasan untuk status spesifik.

RemediationPesan

Saran untuk memperbaiki FAILED status. Misalnya, jika sumber daya tidak memiliki enkripsi, Anda dapat menyatakan cara menambahkan enkripsi ke konfigurasi sumber daya.

RemediationLink

URL HTTP untuk panduan remediasi tambahan.

Tingkat keparahan

Mendefinisikan risiko relatif yang terkait dengan pelanggaran jenis ini. Saat menetapkan tingkat keparahan ke hasil pemanggilan Hook Anda, Anda dapat mereferensikan [kerangka](#)

[AWS Security Hub CSPM keparahan](#) sebagai contoh cara menyusun kategori keparahan yang bermakna.

Nilai yang valid: (INFORMATIONAL| LOW | MEDIUM | HIGH |CRITICAL)

Contoh

Berikut ini adalah contoh respons yang berhasil:

```
{
  "hookStatus": "SUCCESS",
  "message": "compliant",
  "clientRequestToken": "123avjdjk31"
}
```

Berikut ini adalah contoh respons yang gagal:

```
{
  "hookStatus": "FAILED",
  "errorCode": "NonCompliant",
  "message": "S3 Bucket Versioning must be enabled.",
  "clientRequestToken": "123avjdjk31"
}
```

Mengevaluasi operasi sumber daya dengan Lambda Hooks

Setiap kali Anda membuat, memperbarui, atau menghapus sumber daya, itu dianggap sebagai operasi sumber daya. Sebagai contoh, jika Anda menjalankan pembaruan CloudFormation tumpukan yang membuat sumber daya baru, Anda telah menyelesaikan operasi sumber daya. Saat Anda membuat, memperbarui, atau menghapus sumber daya menggunakan Cloud Control API, itu juga dianggap sebagai operasi sumber daya. Anda dapat mengonfigurasi CloudFormation Lambda Hook Anda untuk menargetkan RESOURCE dan CLOUD_CONTROL operasi dalam konfigurasi HookTargetOperations.

Note

deleteHandler Hook hanya dipanggil ketika sumber daya dihapus menggunakan pemicu operasi dari Cloud Control API delete-resource atau CloudFormation delete-stack

Topik

- [Sintaks masukan sumber daya Lambda Hook](#)
- [Contoh input perubahan sumber daya Lambda Hook](#)
- [Contoh fungsi Lambda untuk operasi sumber daya](#)

Sintaks masukan sumber daya Lambda Hook

Ketika Lambda Anda dipanggil untuk operasi sumber daya, Anda akan menerima input JSON yang berisi properti sumber daya, properti yang diusulkan, dan konteks di sekitar pemanggilan Hook.

Berikut ini adalah contoh bentuk input JSON:

```
{
  "awsAccountId": String,
  "stackId": String,
  "changeSetId": String,
  "hookTypeName": String,
  "hookTypeVersion": String,
  "hookModel": {
    "LambdaFunction": String
  },
  "actionInvocationPoint": "CREATE_PRE_PROVISION" or "UPDATE_PRE_PROVISION" or
"DELETE_PRE_PROVISION"
  "requestData": {
    "targetName": String,
    "targetType": String,
    "targetLogicalId": String,
    "targetModel": {
      "resourceProperties": {...},
      "previousResourceProperties": {...}
    }
  },
  "requestContext": {
    "doa": 1,
    "CallbackContext": null
  }
}
```

awsAccountId

ID yang Akun AWS berisi sumber daya yang sedang dievaluasi.

stackId

ID tumpukan CloudFormation tumpukan operasi ini adalah bagian dari. Bidang ini kosong jika penelepon adalah Cloud Control API.

changeSetId

ID dari set perubahan yang memulai pemanggilan Hook. Nilai ini kosong jika perubahan sumber daya dimulai oleh Cloud Control API, atau `create-stackupdate-stack`, atau `delete-stack` operasi.

hookTypeName

Nama Hook yang sedang berjalan.

hookTypeVersion

Versi Hook yang sedang berjalan.

hookModel

`LambdaFunction`

Lambda ARN saat ini dipanggil oleh Hook.

actionInvocationPoint

Poin yang tepat dalam logika penyediaan tempat Hook berjalan.

Nilai yang valid: (`CREATE_PRE_PROVISION`| `UPDATE_PRE_PROVISION` |`DELETE_PRE_PROVISION`)

requestData

`targetName`

Jenis target yang sedang dievaluasi, misalnya, `AWS::S3::Bucket`.

`targetType`

Jenis target yang sedang dievaluasi, misalnya `AWS::S3::Bucket`. Untuk sumber daya yang disediakan dengan Cloud Control API, nilai ini akan menjadi `RESOURCE`

`targetLogicalId`

ID logis dari sumber daya yang sedang dievaluasi. Jika asal pemanggilan Hook adalah CloudFormation, ini akan menjadi ID sumber daya logis yang ditentukan dalam template Anda CloudFormation . Jika asal pemanggilan Hook ini adalah Cloud Control API, ini akan menjadi nilai yang dibangun.

targetModel

resourceProperties

Properti yang diusulkan dari sumber daya yang sedang dimodifikasi. Jika sumber daya dihapus, nilai ini akan kosong.

previousResourceProperties

Properti yang saat ini terkait dengan sumber daya yang sedang dimodifikasi. Jika sumber daya sedang dibuat, nilai ini akan kosong.

requestContext

do

Upaya saat ini untuk mengeksekusi Hook.

CallbackContext

Jika Hook was diatur ke `IN_PROGRESS`, dan dikembalikan, `callbackContext` itu akan ada di sini setelah pemanggilan kembali.

Contoh input perubahan sumber daya Lambda Hook

Contoh input berikut menunjukkan Lambda Hook yang akan menerima definisi

`AWS::DynamoDB::Table` sumber daya untuk memperbarui, di mana dari diubah dari 3 menjadi 10. `ReadCapacityUnits ProvisionedThroughput` Ini adalah data yang tersedia untuk Lambda untuk evaluasi.

```
{
  "awsAccountId": "123456789012",
  "stackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
  "hookTypeName": "my::lambda::resourcehookfunction",
  "hookTypeVersion": "00000008",
  "hookModel": {
    "LambdaFunction": "arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
  },
  "actionInvocationPoint": "UPDATE_PRE_PROVISION",
  "requestData": {
    "targetName": "AWS::DynamoDB::Table",
    "targetType": "AWS::DynamoDB::Table",
    "targetLogicalId": "DDBTable",
    "targetModel": {
```

```
"resourceProperties": {
  "AttributeDefinitions": [
    {
      "AttributeType": "S",
      "AttributeName": "Album"
    },
    {
      "AttributeType": "S",
      "AttributeName": "Artist"
    }
  ],
  "ProvisionedThroughput": {
    "WriteCapacityUnits": 5,
    "ReadCapacityUnits": 10
  },
  "KeySchema": [
    {
      "KeyType": "HASH",
      "AttributeName": "Album"
    },
    {
      "KeyType": "RANGE",
      "AttributeName": "Artist"
    }
  ]
},
"previousResourceProperties": {
  "AttributeDefinitions": [
    {
      "AttributeType": "S",
      "AttributeName": "Album"
    },
    {
      "AttributeType": "S",
      "AttributeName": "Artist"
    }
  ],
  "ProvisionedThroughput": {
    "WriteCapacityUnits": 5,
    "ReadCapacityUnits": 5
  },
  "KeySchema": [
    {
      "KeyType": "HASH",
```

```

        "AttributeName": "Album"
      },
      {
        "KeyType": "RANGE",
        "AttributeName": "Artist"
      }
    ]
  }
},
"requestContext": {
  "invocation": 1,
  "callbackContext": null
}
}

```

Untuk melihat semua properti yang tersedia untuk jenis sumber daya, lihat [AWS::DynamoDB::Table](#).

Contoh fungsi Lambda untuk operasi sumber daya

Berikut ini adalah fungsi sederhana yang gagal setiap pembaruan sumber daya untuk DynamoDB, yang mencoba untuk mengatur ReadCapacity ProvisionedThroughput dari untuk sesuatu yang lebih besar dari 10. Jika Hook berhasil, pesan, "ReadCapacity dikonfigurasi dengan benar," akan ditampilkan ke penelepon. Jika permintaan gagal validasi, Hook akan gagal dengan status, "ReadCapacity tidak boleh lebih dari 10."

Node.js

```

export const handler = async (event, context) => {
  var targetModel = event?.requestData?.targetModel;
  var targetName = event?.requestData?.targetName;
  var response = {
    "hookStatus": "SUCCESS",
    "message": "ReadCapacity is correctly configured.",
    "clientRequestToken": event.clientRequestToken
  };

  if (targetName == "AWS::DynamoDB::Table") {
    var readCapacity =
targetModel?.resourceProperties?.ProvisionedThroughput?.ReadCapacityUnits;
    if (readCapacity > 10) {
      response.hookStatus = "FAILED";
      response.errorCode = "NonCompliant";
    }
  }
}

```

```
        response.message = "ReadCapacity must be cannot be more than 10.";
    }
}
return response;
};
```

Python

```
import json

def lambda_handler(event, context):
    # Using dict.get() for safe access to nested dictionary values
    request_data = event.get('requestData', {})
    target_model = request_data.get('targetModel', {})
    target_name = request_data.get('targetName', '')

    response = {
        "hookStatus": "SUCCESS",
        "message": "ReadCapacity is correctly configured.",
        "clientRequestToken": event.get('clientRequestToken')
    }

    if target_name == "AWS::DynamoDB::Table":
        # Safely navigate nested dictionary
        resource_properties = target_model.get('resourceProperties', {})
        provisioned_throughput = resource_properties.get('ProvisionedThroughput',
        {})

        read_capacity = provisioned_throughput.get('ReadCapacityUnits')

        if read_capacity and read_capacity > 10:
            response['hookStatus'] = "FAILED"
            response['errorCode'] = "NonCompliant"
            response['message'] = "ReadCapacity must be cannot be more than 10."

    return response
```

Mengevaluasi operasi tumpukan dengan Lambda Hooks

Setiap kali Anda membuat, memperbarui, atau menghapus tumpukan dengan templat baru, Anda dapat mengonfigurasi CloudFormation Lambda Hook Anda untuk memulai dengan mengevaluasi template baru dan berpotensi memblokir operasi tumpukan agar tidak dilanjutkan. Anda dapat

mengonfigurasi CloudFormation Lambda Hook Anda untuk menargetkan STACK operasi dalam konfigurasi HookTargetOperations.

Topik

- [Sintaks masukan tumpukan Lambda Hook](#)
- [Contoh input perubahan tumpukan Lambda Hook](#)
- [Contoh fungsi Lambda untuk operasi tumpukan](#)

Sintaks masukan tumpukan Lambda Hook

Saat Lambda Anda dipanggil untuk operasi tumpukan, Anda akan menerima permintaan JSON yang berisi konteks pemanggilan Hook, dan konteks permintaan. `actionInvocationPoint` Karena ukuran CloudFormation template, dan ukuran input terbatas yang diterima oleh fungsi Lambda, template sebenarnya disimpan dalam objek Amazon S3. Masukan `requestData` menyertakan URL Amazon S3 yang mengundurkan diri ke objek lain, yang berisi versi template saat ini dan sebelumnya.

Berikut ini adalah contoh bentuk input JSON:

```
{
  "clientRequestToken": String,
  "awsAccountId": String,
  "stackID": String,
  "changeSetId": String,
  "hookTypeName": String,
  "hookTypeVersion": String,
  "hookModel": {
    "LambdaFunction": String
  },
  "actionInvocationPoint": "CREATE_PRE_PROVISION" or "UPDATE_PRE_PROVISION" or
  "DELETE_PRE_PROVISION"
  "requestData": {
    "targetName": "STACK",
    "targetType": "STACK",
    "targetLogicalId": String,
    "payload": String (S3 Presigned URL)
  },
  "requestContext": {
    "invocation": Integer,
    "callbackContext": String
  }
}
```

```
}  
}
```

clientRequestToken

Token permintaan yang disediakan sebagai masukan untuk permintaan Hook. Bidang ini harus diisi.

awsAccountId

ID yang Akun AWS berisi tumpukan yang sedang dievaluasi.

stackID

ID tumpukan CloudFormation tumpukan.

changeSetId

ID dari set perubahan yang memulai pemanggilan Hook. Nilai ini kosong jika perubahan tumpukan dimulai oleh Cloud Control API, atau `create-stack`, `update-stack`, atau `delete-stack` operasi.

hookTypeName

Nama Hook yang sedang berjalan.

hookTypeVersion

Versi Hook yang sedang berjalan.

hookModel

LambdaFunction

Lambda ARN saat ini dipanggil oleh Hook.

actionInvocationPoint

Poin yang tepat dalam logika penyediaan tempat Hook berjalan.

Nilai yang valid: (CREATE_PRE_PROVISION| UPDATE_PRE_PROVISION
|DELETE_PRE_PROVISION)

requestData

targetName

Nilai ini akan menjadi STACK.

targetType

Nilai ini akan menjadi `STACK`.

targetLogicalId

Nama tumpukan.

payload

URL presigned Amazon S3 yang berisi objek JSON dengan definisi template saat ini dan sebelumnya.

requestContext

Jika Hook sedang dipanggil kembali, objek ini akan diatur.

invocation

Upaya saat ini untuk mengeksekusi Hook.

callbackContext

Jika Hook diatur ke `IN_PROGRESS` dan dikembalikan, `callbackContext` itu akan berada di sini setelah pemanggilan kembali.

`payloadProperti` dalam data permintaan adalah URL yang perlu diambil kode Anda. Setelah menerima URL, Anda mendapatkan objek dengan skema berikut:

```
{
  "template": String,
  "previousTemplate": String
}
```

template

CloudFormation Template lengkap yang disediakan untuk `create-stack` atau `update-stack`. Ini bisa berupa string JSON atau YAML tergantung pada apa yang disediakan. CloudFormation

Dalam `delete-stack` operasi, nilai ini akan kosong.

previousTemplate

CloudFormation Template sebelumnya. Ini bisa berupa string JSON atau YAML tergantung pada apa yang disediakan. CloudFormation

Dalam delete-stack operasi, nilai ini akan kosong.

Contoh input perubahan tumpukan Lambda Hook

Berikut ini adalah contoh input perubahan tumpukan. Hook mengevaluasi perubahan yang memperbarui ObjectLockEnabled ke true, dan menambahkan antrian Amazon SQS:

```
{
  "clientRequestToken": "f8da6d11-b23f-48f4-814c-0fb6a667f50e",
  "awsAccountId": "123456789012",
  "stackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
  "changeSetId": null,
  "hookTypeName": "my::lambda::stackhook",
  "hookTypeVersion": "00000008",
  "hookModel": {
    "LambdaFunction": "arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
  },
  "actionInvocationPoint": "UPDATE_PRE_PROVISION",
  "requestData": {
    "targetName": "STACK",
    "targetType": "STACK",
    "targetLogicalId": "my-cloudformation-stack",
    "payload": "https://s3....."
  },
  "requestContext": {
    "invocation": 1,
    "callbackContext": null
  }
}
```

Ini adalah contoh payload dari requestData:

```
{
  "template": "{\"Resources\":{\"S3Bucket\":{\"Type\":\"AWS::S3::Bucket\", \"Properties\":{\"ObjectLockEnabled\":true}},\"SQSQueue\":{\"Type\":\"AWS::SQS::Queue\", \"Properties\":{\"QueueName\":\"NewQueue\"}}}}",
  "previousTemplate": "{\"Resources\":{\"S3Bucket\":{\"Type\":\"AWS::S3::Bucket\", \"Properties\":{\"ObjectLockEnabled\":false}}}}"
```

Contoh fungsi Lambda untuk operasi tumpukan

Contoh berikut adalah fungsi sederhana yang mengunduh payload operasi stack, mem-parsing template JSON, dan mengembalikan. SUCCESS

Node.js

```
export const handler = async (event, context) => {
  var targetType = event?.requestData?.targetType;
  var payloadUrl = event?.requestData?.payload;

  var response = {
    "hookStatus": "SUCCESS",
    "message": "Stack update is compliant",
    "clientRequestToken": event.clientRequestToken
  };
  try {
    const templateHookPayloadRequest = await fetch(payloadUrl);
    const templateHookPayload = await templateHookPayloadRequest.json()
    if (templateHookPayload.template) {
      // Do something with the template templateHookPayload.template
      // JSON or YAML
    }
    if (templateHookPayload.previousTemplate) {
      // Do something with the template templateHookPayload.previousTemplate
      // JSON or YAML
    }
  } catch (error) {
    console.log(error);
    response.hookStatus = "FAILED";
    response.message = "Failed to evaluate stack operation.";
    response.errorCode = "InternalFailure";
  }
  return response;
};
```

Python

Untuk menggunakan Python, Anda harus mengimpor pustaka. `requests` Untuk melakukan ini, Anda harus menyertakan pustaka dalam paket penyebaran Anda saat membuat fungsi Lambda Anda. Untuk informasi selengkapnya, lihat [Membuat paket deployment .zip dengan dependensi](#) di Panduan Pengembang.AWS Lambda

```
import json
import requests

def lambda_handler(event, context):
    # Safely access nested dictionary values
    request_data = event.get('requestData', {})
    target_type = request_data.get('targetType')
    payload_url = request_data.get('payload')

    response = {
        "hookStatus": "SUCCESS",
        "message": "Stack update is compliant",
        "clientRequestToken": event.get('clientRequestToken')
    }

    try:
        # Fetch the payload
        template_hook_payload_request = requests.get(payload_url)
        template_hook_payload_request.raise_for_status() # Raise an exception for
        bad responses
        template_hook_payload = template_hook_payload_request.json()

        if 'template' in template_hook_payload:
            # Do something with the template template_hook_payload['template']
            # JSON or YAML
            pass

        if 'previousTemplate' in template_hook_payload:
            # Do something with the template
            template_hook_payload['previousTemplate']
            # JSON or YAML
            pass

    except Exception as error:
        print(error)
        response['hookStatus'] = "FAILED"
        response['message'] = "Failed to evaluate stack operation."
        response['errorCode'] = "InternalFailure"

    return response
```

Mengevaluasi operasi set perubahan dengan Lambda Hooks

Setiap kali Anda membuat set perubahan, Anda dapat mengonfigurasi CloudFormation Lambda Hook Anda untuk terlebih dahulu mengevaluasi set perubahan baru dan berpotensi memblokir pelaksanaannya. Anda dapat mengonfigurasi CloudFormation Lambda Hook Anda untuk menargetkan CHANGE_SET operasi dalam konfigurasi HookTargetOperations.

Topik

- [Lambda Hook mengubah sintaks masukan set](#)
- [Contoh perubahan Lambda Hook mengatur masukan perubahan](#)
- [Contoh fungsi Lambda untuk operasi set perubahan](#)

Lambda Hook mengubah sintaks masukan set

Input untuk operasi set perubahan mirip dengan operasi tumpukan, tetapi payload requestData juga mencakup daftar perubahan sumber daya yang diperkenalkan oleh set perubahan.

Berikut ini adalah contoh bentuk input JSON:

```
{
  "clientRequestToken": String,
  "awsAccountId": String,
  "stackID": String,
  "changeSetId": String,
  "hookTypeName": String,
  "hookTypeVersion": String,
  "hookModel": {
    "LambdaFunction": String
  },
  "requestData": {
    "targetName": "CHANGE_SET",
    "targetType": "CHANGE_SET",
    "targetLogicalId": String,
    "payload": String (S3 Presigned URL)
  },
  "requestContext": {
    "invocation": Integer,
    "callbackContext": String
  }
}
```

`clientRequestToken`

Token permintaan yang disediakan sebagai masukan untuk permintaan Hook. Bidang ini harus diisi.

`awsAccountId`

ID yang Akun AWS berisi tumpukan yang sedang dievaluasi.

`stackID`

ID tumpukan CloudFormation tumpukan.

`changeSetId`

ID dari set perubahan yang memulai pemanggilan Hook.

`hookTypeName`

Nama Hook yang sedang berjalan.

`hookTypeVersion`

Versi Hook yang sedang berjalan.

`hookModel`

`LambdaFunction`

Lambda ARN saat ini dipanggil oleh Hook.

`requestData`

`targetName`

Nilai ini akan menjadi `CHANGE_SET`.

`targetType`

Nilai ini akan menjadi `CHANGE_SET`.

`targetLogicalId`

Perubahan set ARN..

`payload`

URL presigned Amazon S3 yang berisi objek JSON dengan template saat ini, serta daftar perubahan yang diperkenalkan oleh set perubahan ini.

requestContext

Jika Hook sedang dipanggil kembali, objek ini akan diatur.

invocation

Upaya saat ini untuk mengeksekusi Hook.

callbackContext

Jika Hook diatur ke `IN_PROGRESS` dan dikembalikan, `callbackContext` itu akan berada di sini setelah pemanggilan kembali.

`payloadProperti` dalam data permintaan adalah URL yang perlu diambil kode Anda. Setelah menerima URL, Anda mendapatkan objek dengan skema berikut:

```
{
  "template": String,
  "changedResources": [
    {
      "action": String,
      "beforeContext": JSON String,
      "afterContext": JSON String,
      "lineNumber": Integer,
      "logicalResourceId": String,
      "resourceType": String
    }
  ]
}
```

template

CloudFormation Template lengkap yang disediakan untuk `create-stack` atau `update-stack`. Ini bisa berupa string JSON atau YAML tergantung pada apa yang disediakan. CloudFormation

changedResources

Daftar sumber daya yang diubah.

action

Jenis perubahan yang diterapkan pada sumber daya.

Nilai yang valid: `(CREATE|UPDATE|DELETE)`

beforeContext

Sebuah string JSON dari properti sumber daya sebelum perubahan. Nilai ini adalah null ketika sumber daya sedang dibuat. Semua nilai boolean dan angka dalam string JSON ini adalah STRINGS.

afterContext

Sebuah string JSON dari properti sumber daya jika set perubahan ini dijalankan. Nilai ini adalah null ketika sumber daya sedang dihapus. Semua nilai boolean dan angka dalam string JSON ini adalah STRINGS.

lineNumber

Nomor baris dalam template yang menyebabkan perubahan ini. Jika tindakan adalah nilai DELETE ini akan menjadi nol.

logicalResourceId

ID sumber daya logis dari sumber daya yang diubah.

resourceType

Jenis sumber daya yang sedang diubah.

Contoh perubahan Lambda Hook mengatur masukan perubahan

Berikut ini adalah contoh perubahan set perubahan input. Dalam contoh berikut, Anda dapat melihat perubahan yang diperkenalkan oleh set perubahan. Perubahan pertama adalah menghapus antrian yang disebut CoolQueue. Perubahan kedua adalah menambahkan antrian baru yang disebut NewCoolQueue. Perubahan terakhir adalah pembaruan ke DynamoDBTable.

```
{
  "clientRequestToken": "f8da6d11-b23f-48f4-814c-0fb6a667f50e",
  "awsAccountId": "123456789012",
  "stackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/
MyStack/1a2345b6-0000-00a0-a123-00abc0abc000",
  "changeSetId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000",
  "hookTypeName": "my::lambda::changesethook",
  "hookTypeVersion": "00000008",
  "hookModel": {
    "LambdaFunction": "arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
  },
}
```

```

    "actionInvocationPoint": "CREATE_PRE_PROVISION",
    "requestData": {
      "targetName": "CHANGE_SET",
      "targetType": "CHANGE_SET",
      "targetLogicalId": "arn:aws:cloudformation:us-west-2:123456789012:changeSet/
SampleChangeSet/1a2345b6-0000-00a0-a123-00abc0abc000",
      "payload": "https://s3....."
    },
    "requestContext": {
      "invocation": 1,
      "callbackContext": null
    }
  }
}

```

Ini adalah contoh payload dari `requestData.payload`:

```

{
  template: 'Resources:\n' +
    '  DynamoDBTable:\n' +
    '    Type: AWS::DynamoDB::Table\n' +
    '    Properties:\n' +
    '      AttributeDefinitions:\n' +
    '        - AttributeName: "PK"\n' +
    '          AttributeType: "S"\n' +
    '      BillingMode: "PAY_PER_REQUEST"\n' +
    '      KeySchema:\n' +
    '        - AttributeName: "PK"\n' +
    '          KeyType: "HASH"\n' +
    '      PointInTimeRecoverySpecification:\n' +
    '        PointInTimeRecoveryEnabled: false\n' +
    '    NewSQSQueue:\n' +
    '      Type: AWS::SQS::Queue\n' +
    '      Properties:\n' +
    '        QueueName: "NewCoolQueue"',
  changedResources: [
    {
      logicalResourceId: 'SQSQueue',
      resourceType: 'AWS::SQS::Queue',
      action: 'DELETE',
      lineNumber: null,
      beforeContext: '{"Properties":{"QueueName":"CoolQueue"}}',
      afterContext: null
    },
  ],
}

```

```

{
  logicalResourceId: 'NewSQSQueue',
  resourceType: 'AWS::SQS::Queue',
  action: 'CREATE',
  lineNumber: 14,
  beforeContext: null,
  afterContext: '{"Properties":{"QueueName":"NewCoolQueue"}}'
},
{
  logicalResourceId: 'DynamoDBTable',
  resourceType: 'AWS::DynamoDB::Table',
  action: 'UPDATE',
  lineNumber: 2,
  beforeContext: '{"Properties":
{"BillingMode":"PAY_PER_REQUEST","AttributeDefinitions":
[{"AttributeType":"S","AttributeName":"PK"}],"KeySchema":
[{"KeyType":"HASH","AttributeName":"PK"}]}' ,
  afterContext: '{"Properties":
{"BillingMode":"PAY_PER_REQUEST","PointInTimeRecoverySpecification":
{"PointInTimeRecoveryEnabled":"false"},"AttributeDefinitions":
[{"AttributeType":"S","AttributeName":"PK"}],"KeySchema":
[{"KeyType":"HASH","AttributeName":"PK"}]}'
}
]
}

```

Contoh fungsi Lambda untuk operasi set perubahan

Contoh berikut adalah fungsi sederhana yang mengunduh payload operasi set perubahan, loop melalui setiap perubahan, dan kemudian mencetak properti sebelum dan sesudah sebelum mengembalikan aSUCCESS.

Node.js

```

export const handler = async (event, context) => {
  var payloadUrl = event?.requestData?.payload;
  var response = {
    "hookStatus": "SUCCESS",
    "message": "Change set changes are compliant",
    "clientRequestToken": event.clientRequestToken
  };
  try {
    const changeSetHookPayloadRequest = await fetch(payloadUrl);

```

```
const changeSetHookPayload = await changeSetHookPayloadRequest.json();
const changes = changeSetHookPayload.changedResources || [];
for(const change of changes) {
  var beforeContext = {};
  var afterContext = {};
  if(change.beforeContext) {
    beforeContext = JSON.parse(change.beforeContext);
  }
  if(change.afterContext) {
    afterContext = JSON.parse(change.afterContext);
  }
  console.log(beforeContext)
  console.log(afterContext)
  // Evaluate Change here
}
} catch (error) {
  console.log(error);
  response.hookStatus = "FAILED";
  response.message = "Failed to evaluate change set operation.";
  response.errorCode = "InternalFailure";
}
return response;
};
```

Python

Untuk menggunakan Python, Anda harus mengimpor pustaka. `requests` Untuk melakukan ini, Anda harus menyertakan pustaka dalam paket penyebaran Anda saat membuat fungsi Lambda Anda. Untuk informasi selengkapnya, lihat [Membuat paket deployment .zip dengan dependensi](#) di Panduan Pengembang.AWS Lambda

```
import json
import requests

def lambda_handler(event, context):
    payload_url = event.get('requestData', {}).get('payload')
    response = {
        "hookStatus": "SUCCESS",
        "message": "Change set changes are compliant",
        "clientRequestToken": event.get('clientRequestToken')
    }

    try:
```

```
change_set_hook_payload_request = requests.get(payload_url)
change_set_hook_payload_request.raise_for_status() # Raises an HTTPError
for bad responses
change_set_hook_payload = change_set_hook_payload_request.json()

changes = change_set_hook_payload.get('changedResources', [])

for change in changes:
    before_context = {}
    after_context = {}

    if change.get('beforeContext'):
        before_context = json.loads(change['beforeContext'])

    if change.get('afterContext'):
        after_context = json.loads(change['afterContext'])

    print(before_context)
    print(after_context)
    # Evaluate Change here

except requests.RequestException as error:
    print(error)
    response['hookStatus'] = "FAILED"
    response['message'] = "Failed to evaluate change set operation."
    response['errorCode'] = "InternalFailure"
except json.JSONDecodeError as error:
    print(error)
    response['hookStatus'] = "FAILED"
    response['message'] = "Failed to parse JSON payload."
    response['errorCode'] = "InternalFailure"

return response
```

Bersiaplah untuk membuat Lambda Hook

Sebelum Anda membuat Lambda Hook, Anda harus menyelesaikan prasyarat berikut:

- Anda harus sudah membuat fungsi Lambda. Untuk informasi selengkapnya, lihat [Buat fungsi Lambda untuk Hooks](#).

- Pengguna atau peran yang membuat Hook harus memiliki izin yang cukup untuk mengaktifkan Hooks. Untuk informasi selengkapnya, lihat [Berikan izin IAM untuk Hooks CloudFormation](#).
- Untuk menggunakan AWS CLI atau SDK untuk membuat Lambda Hook, Anda harus secara manual membuat peran eksekusi dengan izin IAM dan kebijakan kepercayaan CloudFormation untuk memungkinkan memanggil Lambda Hook.

Buat peran eksekusi untuk Lambda Hook

Hook menggunakan peran eksekusi untuk izin yang diperlukan untuk memanggil Hook itu di Akun AWS.

Peran ini dapat dibuat secara otomatis jika Anda membuat Lambda Hook dari Konsol Manajemen AWS; jika tidak, Anda harus membuat peran ini sendiri.

Bagian berikut menunjukkan cara mengatur izin untuk membuat Lambda Hook Anda.

Izin yang diperlukan

Ikuti panduan di [Membuat peran menggunakan kebijakan kepercayaan khusus](#) di Panduan Pengguna IAM untuk membuat peran dengan kebijakan kepercayaan khusus.

Kemudian, selesaikan langkah-langkah berikut untuk mengatur izin Anda:

1. Lampirkan kebijakan hak istimewa minimum berikut ke peran IAM yang ingin Anda gunakan untuk membuat Lambda Hook.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
    }
  ]
}
```

2. Berikan izin Hook Anda untuk mengambil peran dengan menambahkan kebijakan kepercayaan ke peran tersebut. Berikut ini menunjukkan contoh kebijakan kepercayaan yang dapat Anda gunakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "hooks.cloudformation.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Aktifkan Lambda Hook di akun Anda

Topik berikut menunjukkan cara mengaktifkan Lambda Hook di akun Anda, yang membuatnya dapat digunakan di akun dan Wilayah tempat diaktifkan.

Topik

- [Aktifkan Lambda Hook \(konsol\)](#)
- [Aktifkan Lambda Hook \(AWS CLI\)](#)
- [Sumber daya terkait](#)

Aktifkan Lambda Hook (konsol)

Untuk mengaktifkan Lambda Hook untuk digunakan di akun Anda


1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.

2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Anda ingin membuat Hook.
3. Jika Anda belum membuat fungsi Lambda untuk Hook, lakukan hal berikut:
 - Buka [halaman Fungsi](#) di konsol Lambda.
 - Buat fungsi Lambda yang akan Anda gunakan dengan Hook ini, dan kemudian kembali ke prosedur ini. Untuk informasi selengkapnya, lihat [Buat fungsi Lambda untuk mengevaluasi sumber daya untuk Lambda Hooks](#).

Jika Anda telah membuat fungsi Lambda Anda, lanjutkan ke langkah berikutnya.

4. Di panel navigasi di sebelah kiri, pilih Hooks.
5. Pada halaman Hooks, pilih Create a Hook, lalu pilih With Lambda.
6. Untuk nama Hook, pilih salah satu opsi berikut:
 - Berikan nama deskriptif singkat yang akan ditambahkan setelahnya `Private::Lambda::`. Misalnya, jika Anda masuk `MyTestHook`, nama Hook lengkap menjadi `Private::Lambda::MyTestHook`.
 - Berikan nama Hook lengkap (juga disebut alias) menggunakan format ini:
`Provider::ServiceName::HookName`
7. Untuk fungsi Lambda, sediakan fungsi Lambda untuk digunakan dengan Hook ini. Anda dapat menggunakan:
 - Nama Sumber Daya Amazon lengkap (ARN) tanpa akhiran.
 - ARN yang memenuhi syarat dengan versi atau akhiran alias.
8. Untuk target Hook, pilih apa yang akan dievaluasi:
 - Stacks - Mengevaluasi template tumpukan saat pengguna membuat, memperbarui, atau menghapus tumpukan.
 - Sumber Daya - Mengevaluasi perubahan sumber daya individu saat pengguna memperbarui tumpukan.
 - Ubah set - Mengevaluasi pembaruan yang direncanakan saat pengguna membuat set perubahan.
 - Cloud Control API - Mengevaluasi membuat, memperbarui, atau menghapus operasi yang diprakarsai oleh [Cloud Control](#) API.
9. Untuk Tindakan, pilih tindakan mana (buat, perbarui, hapus) yang akan memanggil Hook Anda.

10. Untuk mode Hook, pilih bagaimana Hook merespons ketika fungsi Lambda yang dipanggil oleh Hook mengembalikan respons: FAILED
 - Peringatkan — Mengeluarkan peringatan kepada pengguna tetapi memungkinkan tindakan untuk dilanjutkan. Ini berguna untuk validasi non-kritis atau pemeriksaan informasi.
 - Gagal — Mencegah tindakan dari melanjutkan. Ini berguna untuk menegakkan kepatuhan yang ketat atau kebijakan keamanan.
11. Untuk peran Eksekusi, pilih peran IAM yang diasumsikan Hook untuk memanggil fungsi Lambda Anda. Anda dapat mengizinkan CloudFormation untuk secara otomatis membuat peran eksekusi untuk Anda atau Anda dapat menentukan peran yang telah Anda buat.
12. Pilih Berikutnya.
13. (Opsional) Untuk filter Hook, lakukan hal berikut:
 - a. Untuk filter Sumber Daya, tentukan jenis sumber daya mana yang dapat memanggil Hook. Ini memastikan bahwa Hook hanya dipanggil untuk sumber daya yang relevan.
 - b. Untuk kriteria Pemfilteran, pilih logika untuk menerapkan nama tumpukan dan filter peran tumpukan:
 - Semua nama tumpukan dan peran tumpukan — Hook hanya akan dipanggil ketika semua filter yang ditentukan cocok.
 - Setiap nama tumpukan dan peran tumpukan — Hook akan dipanggil jika setidaknya salah satu filter yang ditentukan cocok.

 Note

Untuk operasi Cloud Control API, semua nama Stack dan filter peran Stack diabaikan.

- c. Untuk nama Stack, sertakan atau keculikan tumpukan tertentu dari pemanggilan Hook.
 - Untuk Sertakan, tentukan nama tumpukan yang akan disertakan. Gunakan ini ketika Anda memiliki satu set kecil tumpukan spesifik yang ingin Anda targetkan. Hanya tumpukan yang ditentukan dalam daftar ini yang akan memanggil Hook.
 - Untuk Kecualikan, tentukan nama tumpukan yang akan dikecualikan. Gunakan ini ketika Anda ingin memanggil Hook di sebagian besar tumpukan tetapi mengecualikan beberapa yang spesifik. Semua tumpukan keculi yang tercantum di sini akan memanggil Hook.

- d. Untuk peran Stack, sertakan atau kecualikan tumpukan tertentu dari pemanggilan Hook berdasarkan peran IAM terkait.
 - Untuk Sertakan, tentukan satu atau beberapa peran IAM ARNs untuk menargetkan tumpukan yang terkait dengan peran ini. Hanya operasi tumpukan yang diprakarsai oleh peran ini yang akan memanggil Hook.
 - Untuk Kecualikan, tentukan satu atau beberapa peran IAM ARNs untuk tumpukan yang ingin Anda kecualikan. Hook akan dipanggil pada semua tumpukan kecuali yang diprakarsai oleh peran yang ditentukan.
14. Pilih Berikutnya.
15. Pada halaman Tinjau dan aktifkan, tinjau pilihan Anda. Untuk membuat perubahan, pilih Edit pada bagian terkait.
16. Saat Anda siap untuk melanjutkan, pilih Activate Hook.

Aktifkan Lambda Hook ()AWS CLI

Sebelum melanjutkan, konfirmasikan bahwa Anda telah membuat fungsi Lambda dan peran eksekusi yang akan Anda gunakan dengan Hook ini. Untuk informasi selengkapnya, lihat [Buat fungsi Lambda untuk mengevaluasi sumber daya untuk Lambda Hooks](#) dan [Buat peran eksekusi untuk Lambda Hook](#).

Untuk mengaktifkan Lambda Hook untuk digunakan di akun Anda ()AWS CLI

1. Untuk mulai mengaktifkan Hook, gunakan [activate-type](#) perintah berikut, ganti placeholder dengan nilai spesifik Anda. Perintah ini mengotorisasi Hook untuk menggunakan peran eksekusi tertentu dari Anda Akun AWS.

```
aws cloudformation activate-type --type HOOK \  
  --type-name AWS::Hooks::LambdaHook \  
  --publisher-id aws-hooks \  
  --execution-role-arn arn:aws:iam::123456789012:role/my-execution-role \  
  --type-name-alias Private::Lambda::MyTestHook \  
  --region us-west-2
```

2. Untuk menyelesaikan pengaktifan Hook, Anda harus mengkonfigurasinya menggunakan file konfigurasi JSON.

Gunakan `cat` perintah untuk membuat file JSON dengan struktur berikut. Untuk informasi selengkapnya, lihat [Referensi sintaks skema konfigurasi hook](#).

```
$ cat > config.json
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "CLOUD_CONTROL"
      ],
      "FailureMode": "WARN",
      "Properties": {
        "LambdaFunction": "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction"
      },
      "TargetFilters": {
        "Actions": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ]
      }
    }
  }
}
```

- `HookInvocationStatus`: Setel `ENABLED` untuk mengaktifkan Hook.
 - `TargetOperations`: Tentukan operasi yang akan dievaluasi oleh Hook.
 - `FailureMode`: Setel ke salah satu `FAIL` atau `WARN`.
 - `LambdaFunction`: Tentukan ARN dari fungsi Lambda.
 - `TargetFilters`: Tentukan jenis tindakan yang akan memanggil Hook.
3. Gunakan [set-type-configuration](#) perintah berikut, bersama dengan file JSON yang Anda buat, untuk menerapkan konfigurasi. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation set-type-configuration \
  --configuration file://config.json \
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \
  --region us-west-2
```

Sumber daya terkait

Kami menyediakan contoh template yang dapat Anda gunakan untuk memahami cara mendeklarasikan Lambda Hook dalam template tumpukan. CloudFormation Untuk informasi selengkapnya, lihat [AWS::CloudFormation::LambdaHook](#) di AWS CloudFormation Panduan Pengguna.

Lihat log untuk Lambda Hooks di akun Anda

Saat menggunakan Lambda Hook, file log laporan keluaran validasi Anda dapat ditemukan di konsol Lambda.

Lihat log Lambda Hook di konsol Lambda

Untuk melihat file log keluaran Lambda Hook

1. Masuk ke konsol Lambda.
2. Pada bilah navigasi di bagian atas layar, pilih Anda Wilayah AWS.
3. Pilih Fungsi.
4. Pilih fungsi Lambda yang diinginkan.
5. Pilih tab Uji.
6. Pilih CloudWatch Log Live Trail
7. Pilih menu tarik-turun dan pilih grup log yang ingin Anda lihat.
8. Pilih Mulai. Log akan ditampilkan di jendela CloudWatch Log Live Trail. Pilih Lihat di kolom atau Lihat dalam teks biasa tergantung pada preferensi Anda.
 - Anda dapat menambahkan lebih banyak filter ke hasil dengan menambahkannya di bidang Add filter pattern. Bidang ini memungkinkan Anda memfilter hasil untuk hanya menyertakan peristiwa yang cocok dengan pola yang ditentukan.

Untuk informasi selengkapnya tentang melihat log untuk fungsi Lambda, lihat [Melihat CloudWatch Log untuk fungsi Lambda](#).

Hapus Lambda Hooks di akun Anda

Bila Anda tidak lagi membutuhkan Lambda Hook yang diaktifkan, gunakan prosedur berikut untuk menghapusnya di akun Anda.

Untuk menonaktifkan sementara Hook alih-alih menghapusnya, lihat [Nonaktifkan dan aktifkan CloudFormation Hooks](#).

Topik

- [Hapus Lambda Hook di akun Anda \(konsol\)](#)
- [Hapus Lambda Hook di akun Anda \(\)AWS CLI](#)

Hapus Lambda Hook di akun Anda (konsol)

Untuk menghapus Lambda Hook di akun Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Hook berada.
3. Dari panel navigasi, pilih Hooks.
4. Pada halaman Hooks, temukan Lambda Hook yang ingin Anda hapus.
5. Pilih kotak centang di sebelah Hook Anda dan pilih Hapus.
6. Saat diminta konfirmasi, ketikkan nama Hook untuk mengonfirmasi penghapusan Hook yang ditentukan dan kemudian pilih Hapus.

Hapus Lambda Hook di akun Anda ()AWS CLI

Note

Sebelum Anda dapat menghapus Hook, Anda harus menonaktifkannya terlebih dahulu. Untuk informasi selengkapnya, lihat [Nonaktifkan dan aktifkan Hook di akun Anda \(AWS CLI\)](#).

Gunakan [deactivate-type](#) perintah berikut untuk menonaktifkan Hook, yang menghapusnya dari akun Anda. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation deactivate-type \  
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \  
  --region us-west-2
```

Mengembangkan Hooks kustom menggunakan CLI CloudFormation

Bagian ini untuk pelanggan yang ingin mengembangkan Hooks khusus dan mendaftarkannya di CloudFormation registri. Ini memberikan gambaran tentang struktur CloudFormation Hooks, dan panduan untuk mengembangkan, mendaftar, menguji, mengelola, dan menerbitkan Hooks Anda sendiri dengan Python atau Java.

Ada tiga langkah utama dalam mengembangkan Hook kustom:

1. Memulai

Untuk mengembangkan Hooks kustom, Anda harus mengkonfigurasi dan menggunakan CloudFormation CLI. Untuk memulai proyek Hook dan file yang diperlukan, gunakan perintah CloudFormation [initCLI](#) dan tentukan bahwa Anda ingin membuat Hook. Untuk informasi selengkapnya, lihat [Memulai proyek CloudFormation Hooks kustom](#).

2. Model

Untuk memodelkan, membuat, dan memvalidasi skema Hook Anda, tentukan Hook, propertinya, dan atributnya.

CloudFormation CLI menciptakan fungsi handler kosong yang sesuai dengan titik pemanggilan Hook tertentu. Tambahkan logika Anda sendiri ke penanganan ini untuk mengontrol apa yang terjadi selama pemanggilan Hook Anda di setiap tahap siklus hidup targetnya. Untuk informasi selengkapnya, lihat [Pemodelan CloudFormation Kait kustom](#).

3. Daftar

Untuk mendaftarkan Hook, kirimkan Hook Anda untuk didaftarkan baik sebagai ekstensi pihak ketiga pribadi atau publik. Daftarkan Hook Anda dengan [submit](#) operasi. Untuk informasi selengkapnya, lihat [Mendaftarkan Hook khusus dengan CloudFormation](#).

Tugas-tugas berikut dikaitkan dengan mendaftarkan Hook Anda:

- a. Publikasikan — Kait dipublikasikan ke registri.
- b. Konfigurasi - Kait dikonfigurasi saat konfigurasi tipe dipanggil terhadap tumpukan.

Note

Kait akan habis waktu setelah 30 detik dan coba lagi hingga 3 kali. Untuk informasi selengkapnya, lihat [Batas batas waktu dan coba lagi](#).

Topik

- [Prasyarat untuk mengembangkan Hooks kustom CloudFormation](#)
- [Memulai proyek CloudFormation Hooks kustom](#)
- [Pemodelan CloudFormation Kait kustom](#)
- [Mendaftarkan Hook khusus dengan CloudFormation](#)
- [Menguji Hook kustom di Akun AWS](#)
- [Memperbarui Hook kustom](#)
- [Membatalkan pendaftaran Hook kustom dari registri CloudFormation](#)
- [Publishing Hooks untuk penggunaan umum](#)
- [Referensi sintaks skema untuk Hooks CloudFormation](#)

Prasyarat untuk mengembangkan Hooks kustom CloudFormation

Anda dapat mengembangkan Hook kustom dengan Java atau Python. Berikut ini adalah prasyarat untuk mengembangkan Hooks kustom:

Prasyarat Java

- [Apache Maven](#)
- [JDK 17](#)

Note

Jika Anda bermaksud menggunakan [CloudFormation Command Line Interface \(CLI\)](#) untuk memulai proyek Hooks untuk Java, Anda harus menginstal Python 3.8 atau yang lebih baru juga. Plugin Java untuk CloudFormation CLI dapat diinstal melalui (manajer paket pip Python), yang distributed dengan Python.

Untuk mengimplementasikan Hook handler untuk proyek Java Hooks Anda, Anda dapat mengunduh file contoh [handler Java Hook](#).

Prasyarat Python

- [Python versi 3.8](#) atau yang lebih baru.

Untuk mengimplementasikan Hook handler untuk proyek Python Hooks Anda, Anda dapat mengunduh file contoh handler [Python Hook](#).

Izin untuk mengembangkan Hooks

Selain izin CloudFormation Create, Update, dan Delete tumpukan, Anda akan memerlukan akses ke AWS CloudFormation operasi berikut. Akses ke operasi ini dikelola melalui CloudFormation kebijakan peran IAM Anda.

- [register-type](#)
- [list-types](#)
- [deregister-type](#)
- [set-type-configuration](#)

Untuk informasi selengkapnya, lihat [Berikan izin IAM untuk Hooks CloudFormation](#).

Menyiapkan lingkungan pengembangan untuk Hooks

Untuk mengembangkan Hooks, Anda harus terbiasa dengan [CloudFormation template](#), dan baik Python atau Java.

Untuk menginstal CloudFormation CLI, dan plugin terkait:

1. Instal CloudFormation CLI dengan pip, manajer paket Python.

```
pip3 install cloudformation-cli
```

2. Instal plugin Python atau Java untuk CLI CloudFormation .

Python

```
pip3 install cloudformation-cli-python-plugin
```

Java

```
pip3 install cloudformation-cli-java-plugin
```

Untuk meng-upgrade CloudFormation CLI dan plugin, Anda dapat menggunakan opsi upgrade.

Python

```
pip3 install --upgrade cloudformation-cli cloudformation-cli-python-plugin
```

Java

```
pip3 install --upgrade cloudformation-cli cloudformation-cli-java-plugin
```

Memulai proyek CloudFormation Hooks kustom

Langkah pertama dalam membuat proyek Hooks kustom Anda adalah memulai proyek. Anda dapat menggunakan `init` perintah CloudFormation CLI untuk memulai proyek Hooks kustom Anda.

`init`Perintah meluncurkan wizard yang memandu Anda melalui pengaturan proyek, termasuk file skema Hooks. Gunakan file skema ini sebagai titik awal untuk menentukan bentuk dan semantik Hooks Anda. Untuk informasi selengkapnya, lihat [Skema sintaks](#).

Untuk memulai proyek Hook:

1. Buat direktori untuk proyek.

```
mkdir ~/mycompany-testing-mytesthook
```

2. Arahkan ke direktori baru.

```
cd ~/mycompany-testing-mytesthook
```

3. Gunakan `init` perintah CloudFormation CLI untuk memulai proyek.

```
cfn init
```

Perintah mengembalikan output berikut.

```
Initializing new project
```

4. `init` Perintah meluncurkan wizard yang memandu Anda melalui pengaturan proyek. Saat diminta, masukkan `h` untuk menentukan proyek Hooks.

```
Do you want to develop a new resource(r) a module(m) or a hook(h)?
```

```
h
```

5. Masukkan nama untuk jenis Hook Anda.

```
What's the name of your hook type?  
(Organization::Service::Hook)
```

```
MyCompany::Testing::MyTestHook
```

6. Jika hanya satu plugin bahasa yang diinstal, itu dipilih secara default. Jika lebih dari satu plugin bahasa diinstal, Anda dapat memilih bahasa yang Anda inginkan. Masukkan pilihan nomor untuk bahasa pilihan Anda.

```
Select a language for code generation:  
[1] java  
[2] python38  
[3] python39  
(enter an integer):
```

7. Siapkan kemasan berdasarkan lanaguage pengembangan yang dipilih.

Python

(Opsional) Pilih Docker untuk kemasan platform-independen. Meskipun Docker tidak diperlukan, sangat disarankan untuk membuat pengemasan lebih mudah.

```
Use docker for platform-independent packaging (Y/n)?
```

```
This is highly recommended unless you are experienced with cross-platform Python packaging.
```

Java

Tetapkan nama paket Java dan pilih model codegen. Anda dapat menggunakan nama paket default, atau membuat yang baru.

Enter a package name (empty for default 'com.mycompany.testing.mytesthook'):

Choose codegen model - 1 (default) or 2 (guided-aws):

Hasil: Anda telah berhasil memulai proyek dan telah menghasilkan file yang diperlukan untuk mengembangkan Hook. Berikut ini adalah contoh direktori dan file yang membentuk proyek Hooks untuk Python 3.8.

```
mycompany-testing-mytesthook.json
rpdk.log
README.md
requirements.txt
hook-role.yaml
template.yml
docs
  README.md
src
  __init__.py
  handlers.py
  models.py
target_models
  aws_s3_bucket.py
```

Note

File dalam `src` direktori dibuat berdasarkan pilihan bahasa Anda. Ada beberapa komentar dan contoh yang berguna dalam file yang dihasilkan. Beberapa file, seperti `models.py`, diperbarui secara otomatis pada langkah selanjutnya ketika Anda menjalankan `generate` perintah untuk menambahkan kode runtime untuk penanganan Anda.

Pemodelan CloudFormation Kait kustom

Pemodelan CloudFormation Hooks kustom melibatkan pembuatan skema yang mendefinisikan Hook, propertinya, dan atributnya. Saat Anda membuat proyek Hook kustom Anda menggunakan `cf n init` perintah, contoh skema Hook dibuat sebagai file teks berformat JSON, `hook-name.json`

Titik pemanggilan target dan tindakan target menentukan titik yang tepat di mana Hook dipanggil. Hook handler menghosting logika kustom yang dapat dieksekusi untuk poin-poin ini. Misalnya, tindakan target CREATE operasi menggunakan `preCreate` handler. Kode Anda yang ditulis dalam handler akan dipanggil saat target dan layanan Hook melakukan tindakan yang cocok. Target hook adalah tujuan di mana kait dipanggil. Anda dapat menentukan target seperti, sumber daya CloudFormation publik, sumber daya pribadi, atau sumber daya khusus. Hooks mendukung jumlah target Hook yang tidak terbatas.

Skema berisi izin yang diperlukan untuk Hook. Menulis Hook mengharuskan Anda untuk menentukan izin untuk setiap handler Hook. CloudFormation mendorong penulis untuk menulis kebijakan yang mengikuti saran keamanan standar untuk memberikan hak istimewa paling sedikit, atau hanya memberikan izin yang diperlukan untuk melakukan tugas. Tentukan apa yang perlu dilakukan pengguna (dan peran), lalu buat kebijakan yang memungkinkan mereka hanya melakukan tugas-tugas tersebut untuk operasi Hook. CloudFormation menggunakan izin ini untuk mencakup-down izin yang diberikan pengguna Hook. Izin ini diteruskan ke Hook. Hook handler menggunakan izin ini untuk mengakses AWS sumber daya.

Anda dapat menggunakan file skema berikut sebagai titik awal untuk menentukan Hook Anda. Gunakan skema Hook untuk menentukan penanganan mana yang ingin Anda terapkan. Jika Anda memilih untuk tidak menerapkan handler tertentu, hapus dari bagian penanganan skema Hook. Untuk detail lebih lanjut tentang skema, lihat [Skema sintaks](#).

```
{
  "typeName": "MyCompany::Testing::MyTestHook",
  "description": "Verifies S3 bucket and SQS queues properties before create and
update",
  "sourceUrl": "https://mycorp.com/my-repo.git",
  "documentationUrl": "https://mycorp.com/documentation",
  "typeConfiguration": {
    "properties": {
      "minBuckets": {
        "description": "Minimum number of compliant buckets",
        "type": "string"
      }
    }
  },
}
```

```
    "minQueues":{
      "description":"Minimum number of compliant queues",
      "type":"string"
    },
    "encryptionAlgorithm":{
      "description":"Encryption algorithm for SSE",
      "default":"AES256",
      "type":"string"
    }
  },
  "required":[

  ],
  "additionalProperties":false
},
"handlers":{
  "preCreate":{
    "targetNames":[
      "AWS::S3::Bucket",
      "AWS::SQS::Queue"
    ],
    "permissions":[

    ]
  },
  "preUpdate":{
    "targetNames":[
      "AWS::S3::Bucket",
      "AWS::SQS::Queue"
    ],
    "permissions":[

    ]
  },
  "preDelete":{
    "targetNames":[
      "AWS::S3::Bucket",
      "AWS::SQS::Queue"
    ],
    "permissions":[
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:GetEncryptionConfiguration",
      "sqs:ListQueues",
```

```
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
    ]
}
},
"additionalProperties":false
}
```

Topik

- [Pemodelan CloudFormation Hooks kustom menggunakan Java](#)
- [Pemodelan CloudFormation Hooks kustom menggunakan Python](#)

Pemodelan CloudFormation Hooks kustom menggunakan Java

Pemodelan CloudFormation Hooks kustom melibatkan pembuatan skema yang mendefinisikan Hook, propertinya, dan atributnya. Tutorial ini memandu Anda melalui pemodelan Hooks kustom menggunakan Java.

Langkah 1: Tambahkan dependensi proyek

Proyek Hooks berbasis Java mengandalkan pom.xml file Maven sebagai dependensi. Perluas bagian berikut dan salin kode sumber ke pom.xml file di root proyek.

Ketergantungan proyek hook (pom.xml)

```
<?xml version="1.0" encoding="UTF-8"?>
<project
  xmlns="http://maven.apache.org/POM/4.0.0"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>

  <groupId>com.mycompany.testing.mytesthook</groupId>
  <artifactId>mycompany-testing-mytesthook-handler</artifactId>
  <name>mycompany-testing-mytesthook-handler</name>
  <version>1.0-SNAPSHOT</version>
  <packaging>jar</packaging>

  <properties>
    <maven.compiler.source>1.8</maven.compiler.source>
```

```
<maven.compiler.target>1.8</maven.compiler.target>
<project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
<project.reporting.outputEncoding>UTF-8</project.reporting.outputEncoding>
<aws.java.sdk.version>2.16.1</aws.java.sdk.version>
<checkstyle.version>8.36.2</checkstyle.version>
<commons-io.version>2.8.0</commons-io.version>
<jackson.version>2.11.3</jackson.version>
<maven-checkstyle-plugin.version>3.1.1</maven-checkstyle-plugin.version>
<mockito.version>3.6.0</mockito.version>
<spotbugs.version>4.1.4</spotbugs.version>
<spotless.version>2.5.0</spotless.version>
<maven-javadoc-plugin.version>3.2.0</maven-javadoc-plugin.version>
<maven-source-plugin.version>3.2.1</maven-source-plugin.version>
<cfm.generate.args/>
</properties>

<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>software.amazon.awssdk</groupId>
      <artifactId>bom</artifactId>
      <version>2.16.1</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
  </dependencies>
</dependencyManagement>

<dependencies>
  <!-- https://mvnrepository.com/artifact/software.amazon.cloudformation/aws-
cloudformation-rpdk-java-plugin -->
  <dependency>
    <groupId>software.amazon.cloudformation</groupId>
    <artifactId>aws-cloudformation-rpdk-java-plugin</artifactId>
    <version>[2.0.0,3.0.0)</version>
  </dependency>

  <!-- AWS Java SDK v2 Dependencies -->
  <dependency>
    <groupId>software.amazon.awssdk</groupId>
    <artifactId>sdk-core</artifactId>
  </dependency>
  <dependency>
    <groupId>software.amazon.awssdk</groupId>
```

```
        <artifactId>cloudformation</artifactId>
    </dependency>
    <dependency>
        <groupId>software.amazon.awssdk</groupId>
        <artifactId>s3</artifactId>
    </dependency>
    <dependency>
        <groupId>software.amazon.awssdk</groupId>
        <artifactId>utils</artifactId>
    </dependency>
    <dependency>
        <groupId>software.amazon.awssdk</groupId>
        <artifactId>apache-client</artifactId>
    </dependency>
    <dependency>
        <groupId>software.amazon.awssdk</groupId>
        <artifactId>sqs</artifactId>
    </dependency>

    <!-- Test dependency for Java Providers -->
    <dependency>
        <groupId>software.amazon.cloudformation</groupId>
        <artifactId>cloudformation-cli-java-plugin-testing-support</artifactId>
        <version>1.0.0</version>
    </dependency>

    <!-- https://mvnrepository.com/artifact/com.amazonaws/aws-java-sdk-s3 -->
    <dependency>
        <groupId>com.amazonaws</groupId>
        <artifactId>aws-java-sdk-s3</artifactId>
        <version>1.12.85</version>
    </dependency>

    <!-- https://mvnrepository.com/artifact/commons-io/commons-io -->
    <dependency>
        <groupId>commons-io</groupId>
        <artifactId>commons-io</artifactId>
        <version>${commons-io.version}</version>
    </dependency>
    <!-- https://mvnrepository.com/artifact/org.apache.commons/commons-lang3 -->
    <dependency>
        <groupId>org.apache.commons</groupId>
        <artifactId>commons-lang3</artifactId>
        <version>3.9</version>
```

```
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.commons/commons-collections4
-->
<dependency>
  <groupId>org.apache.commons</groupId>
  <artifactId>commons-collections4</artifactId>
  <version>4.4</version>
</dependency>
<!-- https://mvnrepository.com/artifact/com.google.guava/guava -->
<dependency>
  <groupId>com.google.guava</groupId>
  <artifactId>guava</artifactId>
  <version>29.0-jre</version>
</dependency>
<!-- https://mvnrepository.com/artifact/com.amazonaws/aws-java-sdk-
cloudformation -->
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-cloudformation</artifactId>
  <version>1.11.555</version>
  <scope>test</scope>
</dependency>

<!-- https://mvnrepository.com/artifact/commons-codec/commons-codec -->
<dependency>
  <groupId>commons-codec</groupId>
  <artifactId>commons-codec</artifactId>
  <version>1.14</version>
</dependency>
<!-- https://mvnrepository.com/artifact/software.amazon.cloudformation/aws-
cloudformation-resource-schema -->
<dependency>
  <groupId>software.amazon.cloudformation</groupId>
  <artifactId>aws-cloudformation-resource-schema</artifactId>
  <version>[2.0.5, 3.0.0)</version>
</dependency>
<!-- https://mvnrepository.com/artifact/com.fasterxml.jackson.dataformat/
jackson-databind -->
<dependency>
  <groupId>com.fasterxml.jackson.core</groupId>
  <artifactId>jackson-databind</artifactId>
  <version>${jackson.version}</version>
</dependency>
```

```
    <!-- https://mvnrepository.com/artifact/com.fasterxml.jackson.dataformat/
jackson-dataformat-cbor -->
    <dependency>
      <groupId>com.fasterxml.jackson.dataformat</groupId>
      <artifactId>jackson-dataformat-cbor</artifactId>
      <version>${jackson.version}</version>
    </dependency>

    <dependency>
      <groupId>com.fasterxml.jackson.datatype</groupId>
      <artifactId>jackson-datatype-jsr310</artifactId>
      <version>${jackson.version}</version>
    </dependency>

    <!-- https://mvnrepository.com/artifact/com.fasterxml.jackson.module/jackson-
modules-java8 -->
    <dependency>
      <groupId>com.fasterxml.jackson.module</groupId>
      <artifactId>jackson-modules-java8</artifactId>
      <version>${jackson.version}</version>
      <type>pom</type>
      <scope>runtime</scope>
    </dependency>

    <!-- https://mvnrepository.com/artifact/org.json/json -->
    <dependency>
      <groupId>org.json</groupId>
      <artifactId>json</artifactId>
      <version>20180813</version>
    </dependency>
    <!-- https://mvnrepository.com/artifact/com.amazonaws/aws-java-sdk-core -->
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-java-sdk-core</artifactId>
      <version>1.11.1034</version>
    </dependency>
    <!-- https://mvnrepository.com/artifact/com.amazonaws/aws-lambda-java-core -->
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-core</artifactId>
      <version>1.2.0</version>
    </dependency>
    <!-- https://mvnrepository.com/artifact/com.amazonaws/aws-lambda-java-log4j2 --
>
```

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-lambda-java-log4j2</artifactId>
  <version>1.2.0</version>
</dependency>

<!-- https://mvnrepository.com/artifact/com.google.code.gson/gson -->
<dependency>
  <groupId>com.google.code.gson</groupId>
  <artifactId>gson</artifactId>
  <version>2.8.8</version>
</dependency>

<!-- https://mvnrepository.com/artifact/org.projectlombok/lombok -->
<dependency>
  <groupId>org.projectlombok</groupId>
  <artifactId>lombok</artifactId>
  <version>1.18.4</version>
  <scope>provided</scope>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-api -->
<dependency>
  <groupId>org.apache.logging.log4j</groupId>
  <artifactId>log4j-api</artifactId>
  <version>2.17.1</version>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-core -->
>
<dependency>
  <groupId>org.apache.logging.log4j</groupId>
  <artifactId>log4j-core</artifactId>
  <version>2.17.1</version>
</dependency>
<!-- https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-slf4j-impl -->
impl -->
<dependency>
  <groupId>org.apache.logging.log4j</groupId>
  <artifactId>log4j-slf4j-impl</artifactId>
  <version>2.17.1</version>
</dependency>

<!-- https://mvnrepository.com/artifact/org.assertj/assertj-core -->
<dependency>
```

```
        <groupId>org.assertj</groupId>
        <artifactId>assertj-core</artifactId>
        <version>3.12.2</version>
        <scope>test</scope>
    </dependency>
    <!-- https://mvnrepository.com/artifact/org.junit.jupiter/junit-jupiter -->
    <dependency>
        <groupId>org.junit.jupiter</groupId>
        <artifactId>junit-jupiter</artifactId>
        <version>5.5.0-M1</version>
        <scope>test</scope>
    </dependency>
    <!-- https://mvnrepository.com/artifact/org.mockito/mockito-core -->
    <dependency>
        <groupId>org.mockito</groupId>
        <artifactId>mockito-core</artifactId>
        <version>3.6.0</version>
        <scope>test</scope>
    </dependency>
    <!-- https://mvnrepository.com/artifact/org.mockito/mockito-junit-jupiter -->
    <dependency>
        <groupId>org.mockito</groupId>
        <artifactId>mockito-junit-jupiter</artifactId>
        <version>3.6.0</version>
        <scope>test</scope>
    </dependency>
</dependencies>

<build>
    <plugins>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-compiler-plugin</artifactId>
            <version>3.8.1</version>
            <configuration>
                <compilerArgs>
                    <arg>-Xlint:all, -options, -processing</arg>
                </compilerArgs>
            </configuration>
        </plugin>
        <plugin>
            <groupId>org.apache.maven.plugins</groupId>
            <artifactId>maven-shade-plugin</artifactId>
            <version>2.3</version>
```

```

    <configuration>
      <createDependencyReducedPom>>false</createDependencyReducedPom>
      <filters>
        <filter>
          <artifact>*:*</artifact>
          <excludes>
            <exclude>**/Log4j2Plugins.dat</exclude>
          </excludes>
        </filter>
      </filters>
    </configuration>
  </executions>
  <execution>
    <phase>package</phase>
    <goals>
      <goal>shade</goal>
    </goals>
  </execution>
</executions>
</plugin>
<plugin>
  <groupId>org.codehaus.mojo</groupId>
  <artifactId>exec-maven-plugin</artifactId>
  <version>1.6.0</version>
  <executions>
    <execution>
      <id>generate</id>
      <phase>generate-sources</phase>
      <goals>
        <goal>exec</goal>
      </goals>
      <configuration>
        <executable>cfn</executable>
        <commandlineArgs>generate ${cfn.generate.args}</
commandlineArgs>
        <workingDirectory>${project.basedir}</workingDirectory>
      </configuration>
    </execution>
  </executions>
</plugin>
<plugin>
  <groupId>org.codehaus.mojo</groupId>
  <artifactId>build-helper-maven-plugin</artifactId>
  <version>3.0.0</version>

```

```

        <executions>
            <execution>
                <id>add-source</id>
                <phase>generate-sources</phase>
                <goals>
                    <goal>add-source</goal>
                </goals>
                <configuration>
                    <sources>
                        <source>${project.basedir}/target/generated-sources/
rpdk</source>
                    </sources>
                </configuration>
            </execution>
        </executions>
    </plugin>
    <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-resources-plugin</artifactId>
        <version>2.4</version>
    </plugin>
    <plugin>
        <artifactId>maven-surefire-plugin</artifactId>
        <version>3.0.0-M3</version>
    </plugin>
    <plugin>
        <groupId>org.jacoco</groupId>
        <artifactId>jacoco-maven-plugin</artifactId>
        <version>0.8.4</version>
        <configuration>
            <excludes>
                <exclude>**/BaseHookConfiguration*</exclude>
                <exclude>**/BaseHookHandler*</exclude>
                <exclude>**/HookHandlerWrapper*</exclude>
                <exclude>**/ResourceModel*</exclude>
                <exclude>**/TypeConfigurationModel*</exclude>
                <exclude>**/model/**/*</exclude>
            </excludes>
        </configuration>
    </plugin>
    <executions>
        <execution>
            <goals>
                <goal>prepare-agent</goal>
            </goals>
    </executions>

```

```
        </execution>
        <execution>
            <id>report</id>
            <phase>test</phase>
            <goals>
                <goal>report</goal>
            </goals>
        </execution>
        <execution>
            <id>jacoco-check</id>
            <goals>
                <goal>check</goal>
            </goals>
            <configuration>
                <rules>
                    <rule>
                        <element>PACKAGE</element>
                        <limits>
                            <limit>
                                <counter>BRANCH</counter>
                                <value>COVEREDRATIO</value>
                                <minimum>0.8</minimum>
                            </limit>
                            <limit>
                                <counter>INSTRUCTION</counter>
                                <value>COVEREDRATIO</value>
                                <minimum>0.8</minimum>
                            </limit>
                        </limits>
                    </rule>
                </rules>
            </configuration>
        </execution>
    </executions>
</plugin>
</plugins>
<resources>
    <resource>
        <directory>${project.basedir}</directory>
        <includes>
            <include>mycompany-testing-mytesthook.json</include>
        </includes>
    </resource>
</resources>
```

```
        <directory>${project.basedir}/target/loaded-target-schemas</directory>
        <includes>
            <include>**/*.json</include>
        </includes>
    </resource>
</resources>
</build>
</project>
```

Langkah 2: Buat paket proyek Hook

Hasilkan paket proyek Hook Anda. CloudFormation CLI menciptakan fungsi handler kosong yang sesuai dengan tindakan Hook tertentu dalam siklus hidup target seperti yang didefinisikan dalam spesifikasi Hook.

```
cfn generate
```

Perintah mengembalikan output berikut.

```
Generated files for MyCompany::Testing::MyTestHook
```

Note

Pastikan runtime Lambda Anda up-to-date untuk menghindari penggunaan versi usang. Untuk informasi selengkapnya, lihat [Memperbarui runtime Lambda untuk jenis sumber daya dan Hooks](#).

Langkah 3: Tambahkan Hook handler

Tambahkan kode runtime Hook handler Anda sendiri ke handler yang Anda pilih untuk diterapkan. Misalnya, Anda dapat menambahkan kode berikut untuk logging.

```
logger.log("Internal testing Hook triggered for target: " +
    request.getHookContext().getTargetName());
```

CloudFormation CLI menghasilkan Plain Old Java Objects (Java POJO). Berikut ini adalah contoh keluaran yang dihasilkan dari `AWS::S3::Bucket`.

Example awSS3 BucketTargetModel .java

```
package com.mycompany.testing.mytesthook.model.aws.s3.bucket;

import...

@Data
@NoArgsConstructor
@EqualsAndHashCode(callSuper = true)
@ToString(callSuper = true)
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class AwsS3BucketTargetModel extends ResourceHookTargetModel<AwsS3Bucket> {

    @JsonIgnore
    private static final TypeReference<AwsS3Bucket> TARGET_REFERENCE =
        new TypeReference<AwsS3Bucket>() {};

    @JsonIgnore
    private static final TypeReference<AwsS3BucketTargetModel> MODEL_REFERENCE =
        new TypeReference<AwsS3BucketTargetModel>() {};

    @JsonIgnore
    public static final String TARGET_TYPE_NAME = "AWS::S3::Bucket";

    @JsonIgnore
    public TypeReference<AwsS3Bucket> getHookTargetTypeReference() {
        return TARGET_REFERENCE;
    }

    @JsonIgnore
    public TypeReference<AwsS3BucketTargetModel> getTargetModelTypeReference() {
        return MODEL_REFERENCE;
    }
}
```

Example AwsS3Bucket.java

```
package com.mycompany.testing.mytesthook.model.aws.s3.bucket;

import ...
```

```
@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
@EqualsAndHashCode(callSuper = true)
@ToString(callSuper = true)
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class AwsS3Bucket extends ResourceHookTarget {
    @JsonIgnore
    public static final String TYPE_NAME = "AWS::S3::Bucket";

    @JsonIgnore
    public static final String IDENTIFIER_KEY_ID = "/properties/Id";

    @JsonProperty("InventoryConfigurations")
    private List<InventoryConfiguration> inventoryConfigurations;

    @JsonProperty("WebsiteConfiguration")
    private WebsiteConfiguration websiteConfiguration;

    @JsonProperty("DualStackDomainName")
    private String dualStackDomainName;

    @JsonProperty("AccessControl")
    private String accessControl;

    @JsonProperty("AnalyticsConfigurations")
    private List<AnalyticsConfiguration> analyticsConfigurations;

    @JsonProperty("AccelerateConfiguration")
    private AccelerateConfiguration accelerateConfiguration;

    @JsonProperty("PublicAccessBlockConfiguration")
    private PublicAccessBlockConfiguration publicAccessBlockConfiguration;

    @JsonProperty("BucketName")
    private String bucketName;

    @JsonProperty("RegionalDomainName")
    private String regionalDomainName;
```

```
@JsonProperty("OwnershipControls")
private OwnershipControls ownershipControls;

@JsonProperty("ObjectLockConfiguration")
private ObjectLockConfiguration objectLockConfiguration;

@JsonProperty("ObjectLockEnabled")
private Boolean objectLockEnabled;

@JsonProperty("LoggingConfiguration")
private LoggingConfiguration loggingConfiguration;

@JsonProperty("ReplicationConfiguration")
private ReplicationConfiguration replicationConfiguration;

@JsonProperty("Tags")
private List<Tag> tags;

@JsonProperty("DomainName")
private String domainName;

@JsonProperty("BucketEncryption")
private BucketEncryption bucketEncryption;

@JsonProperty("WebsiteURL")
private String websiteURL;

@JsonProperty("NotificationConfiguration")
private NotificationConfiguration notificationConfiguration;

@JsonProperty("LifecycleConfiguration")
private LifecycleConfiguration lifecycleConfiguration;

@JsonProperty("VersioningConfiguration")
private VersioningConfiguration versioningConfiguration;

@JsonProperty("MetricsConfigurations")
private List<MetricsConfiguration> metricsConfigurations;

@JsonProperty("IntelligentTieringConfigurations")
private List<IntelligentTieringConfiguration> intelligentTieringConfigurations;

@JsonProperty("CorsConfiguration")
private CorsConfiguration corsConfiguration;
```

```

@JsonProperty("Id")
private String id;

@JsonProperty("Arn")
private String arn;

@JsonIgnore
public JSONObject getPrimaryIdentifier() {
    final JSONObject identifier = new JSONObject();
    if (this.getId() != null) {
        identifier.put(IDENTIFIER_KEY_ID, this.getId());
    }

    // only return the identifier if it can be used, i.e. if all components are
    present
    return identifier.length() == 1 ? identifier : null;
}

@JsonIgnore
public List<JSONObject> getAdditionalIdentifiers() {
    final List<JSONObject> identifiers = new ArrayList<JSONObject>();
    // only return the identifiers if any can be used
    return identifiers.isEmpty() ? null : identifiers;
}
}

```

Example BucketEncryption.jawa

```

package software.amazon.testing.mytesthook.model.aws.s3.bucket;

import ...

@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class BucketEncryption {
    @JsonProperty("ServerSideEncryptionConfiguration")
    private List<ServerSideEncryptionRule> serverSideEncryptionConfiguration;
}

```

```
}
```

Example ServerSideEncryptionRule.java

```
package com.mycompany.testing.mytesthook.model.aws.s3.bucket;

import ...

@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class ServerSideEncryptionRule {
    @JsonProperty("BucketKeyEnabled")
    private Boolean bucketKeyEnabled;

    @JsonProperty("ServerSideEncryptionByDefault")
    private ServerSideEncryptionByDefault serverSideEncryptionByDefault;
}
```

Example ServerSideEncryptionByDefault.java

```
package com.mycompany.testing.mytesthook.model.aws.s3.bucket;

import ...

@Data
@Builder
@AllArgsConstructor
@NoArgsConstructor
@JsonAutoDetect(fieldVisibility = Visibility.ANY, getterVisibility = Visibility.NONE,
    setterVisibility = Visibility.NONE)
public class ServerSideEncryptionByDefault {
    @JsonProperty("SSEAlgorithm")
    private String sSEAlgorithm;

    @JsonProperty("KMSTMasterKeyID")
```

```
private String kmsMasterKeyID;  
  
}
```

Dengan yang POJOs dihasilkan, Anda sekarang dapat menulis penanganan yang benar-benar mengimplementasikan fungsionalitas Hook. Untuk contoh ini, terapkan titik `preCreate` dan `preUpdate` pemanggilan untuk penanganan.

Langkah 4: Menerapkan Hook handler

Topik

- [Mengkodekan pembangun klien API](#)
- [Mengkodekan pembuat permintaan API](#)
- [Menerapkan kode pembantu](#)
- [Menerapkan base handler](#)
- [Menerapkan preCreate handler](#)
- [Mengkodekan preCreate handler](#)
- [Memperbarui preCreate tes](#)
- [Menerapkan preUpdate handler](#)
- [Mengkodekan preUpdate handler](#)
- [Memperbarui preUpdate tes](#)
- [Menerapkan preDelete handler](#)
- [Mengkodekan preDelete handler](#)
- [Memperbarui preDelete handler](#)

Mengkodekan pembangun klien API

1. Di IDE Anda, buka `ClientBuilder.java` file, yang terletak di `src/main/java/com/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `ClientBuilder.java` file dengan kode berikut.

Example ClientBuilder.java

```
package com.awscommunity.kms.encryptionsettings;  
  
import software.amazon.awssdk.services.ec2.Ec2Client;
```

```
import software.amazon.cloudformation.HookLambdaWrapper;

/**
 * Describes static HTTP clients (to consume less memory) for API calls that
 * this hook makes to a number of AWS services.
 */
public final class ClientBuilder {

    private ClientBuilder() {
    }

    /**
     * Create an HTTP client for Amazon EC2.
     *
     * @return Ec2Client An {@link Ec2Client} object.
     */
    public static Ec2Client getEc2Client() {
        return
        Ec2Client.builder().httpClient(HookLambdaWrapper.HTTP_CLIENT).build();
    }
}
```

Mengkodekan pembuat permintaan API

1. Di IDE Anda, buka `Translator.java` file, yang terletak di `src/main/java/com/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `Translator.java` file dengan kode berikut.

Example Translator.java

```
package com.mycompany.testing.mytesthook;

import software.amazon.awssdk.services.s3.model.GetBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesRequest;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

/**
 * This class is a centralized placeholder for
 * - api request construction
 * - object translation to/from aws sdk
 */
```

```
*/  
  
public class Translator {  
  
    static ListBucketsRequest translateToListBucketsRequest(final HookTargetModel  
targetModel) {  
        return ListBucketsRequest.builder().build();  
    }  
  
    static ListQueuesRequest translateToListQueuesRequest(final String nextToken) {  
        return ListQueuesRequest.builder().nextToken(nextToken).build();  
    }  
  
    static ListBucketsRequest createListBucketsRequest() {  
        return ListBucketsRequest.builder().build();  
    }  
  
    static ListQueuesRequest createListQueuesRequest() {  
        return createListQueuesRequest(null);  
    }  
  
    static ListQueuesRequest createListQueuesRequest(final String nextToken) {  
        return ListQueuesRequest.builder().nextToken(nextToken).build();  
    }  
  
    static GetBucketEncryptionRequest createGetBucketEncryptionRequest(final String  
bucket) {  
        return GetBucketEncryptionRequest.builder().bucket(bucket).build();  
    }  
}
```

Menerapkan kode pembantu

1. Di IDE Anda, buka `AbstractTestBase.java` file, yang terletak di `src/main/java/com/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `AbstractTestBase.java` file dengan kode berikut.

Example Translator.java

```
package com.mycompany.testing.mytesthook;  
  
import com.google.common.collect.ImmutableMap;
```

```
import org.mockito.Mockito;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.auth.credentials.AwsSessionCredentials;
import software.amazon.awssdk.auth.credentials.StaticCredentialsProvider;
import software.amazon.awssdk.awscore.AwsRequest;
import software.amazon.awssdk.awscore.AwsRequestOverrideConfiguration;
import software.amazon.awssdk.awscore.AwsResponse;
import software.amazon.awssdk.core.SdkClient;
import software.amazon.awssdk.core.pagination.sync.SdkIterable;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.Credentials;
import software.amazon.cloudformation.proxy.LoggerProxy;
import software.amazon.cloudformation.proxy.OperationStatus;
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.ProxyClient;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import javax.annotation.Nonnull;
import java.time.Duration;
import java.util.concurrent.CompletableFuture;
import java.util.function.Function;
import java.util.function.Supplier;

import static org.assertj.core.api.Assertions.assertThat;

@lombok.Getter
public class AbstractTestBase {
    protected final AwsSessionCredentials awsSessionCredential;
    protected final AwsCredentialsProvider v2CredentialsProvider;
    protected final AwsRequestOverrideConfiguration configuration;
    protected final LoggerProxy loggerProxy;
    protected final Supplier<Long> awsLambdaRuntime = () ->
Duration.ofMinutes(15).toMillis();
    protected final AmazonWebServicesClientProxy proxy;
    protected final Credentials mockCredentials =
        new Credentials("mockAccessId", "mockSecretKey", "mockSessionToken");

    @lombok.Setter
    private SdkClient serviceClient;

    protected AbstractTestBase() {
        loggerProxy = Mockito.mock(LoggerProxy.class);
        awsSessionCredential =
AwsSessionCredentials.create(mockCredentials.getAccessKeyId(),
```

```

        mockCredentials.getSecretAccessKey(),
mockCredentials.getSessionToken());
        v2CredentialsProvider =
StaticCredentialsProvider.create(awsSessionCredential);
        configuration = AwsRequestOverrideConfiguration.builder()
                .credentialsProvider(v2CredentialsProvider)
                .build();
        proxy = new AmazonWebServicesClientProxy(
                loggerProxy,
                mockCredentials,
                awsLambdaRuntime
        ) {
            @Override
            public <ClientT> ProxyClient<ClientT> newProxy(@NonNull
Supplier<ClientT> client) {
                return new ProxyClient<ClientT>() {
                    @Override
                    public <RequestT extends AwsRequest, ResponseT extends
AwsResponse>
                        ResponseT injectCredentialsAndInvokeV2(RequestT request,
Function<RequestT,
ResponseT> requestFunction) {
                            return proxy.injectCredentialsAndInvokeV2(request,
requestFunction);
                        }

                    @Override
                    public <RequestT extends AwsRequest, ResponseT extends
AwsResponse> CompletableFuture<ResponseT>
                        injectCredentialsAndInvokeV2Async(RequestT request,
Function<RequestT, CompletableFuture<ResponseT>> requestFunction) {
                            return proxy.injectCredentialsAndInvokeV2Async(request,
requestFunction);
                        }

                    @Override
                    public <RequestT extends AwsRequest, ResponseT extends
AwsResponse, IterableT extends SdkIterable<ResponseT>>
                        IterableT
                            injectCredentialsAndInvokeIterableV2(RequestT request,
Function<RequestT, IterableT> requestFunction) {
                                return proxy.injectCredentialsAndInvokeIterableV2(request,
requestFunction);
                            }
                }
            }
        }

```

```
        @SuppressWarnings("unchecked")
        @Override
        public ClientT client() {
            return (ClientT) serviceClient;
        }
    };
}

protected void assertResponse(final ProgressEvent<HookTargetModel,
    CallbackContext> response, final OperationStatus expectedStatus, final String
    expectedMsg) {
    assertThat(response).isNotNull();
    assertThat(response.getStatus()).isEqualTo(expectedStatus);
    assertThat(response.getCallbackContext()).isNull();
    assertThat(response.getCallbackDelaySeconds()).isEqualTo(0);
    assertThat(response.getMessage()).isNotNull();
    assertThat(response.getMessage()).isEqualTo(expectedMsg);
}

protected HookTargetModel createHookTargetModel(final Object
    resourceProperties) {
    return HookTargetModel.of(ImmutableMap.of("ResourceProperties",
    resourceProperties));
}

protected HookTargetModel createHookTargetModel(final Object
    resourceProperties, final Object previousResourceProperties) {
    return HookTargetModel.of(
        ImmutableMap.of(
            "ResourceProperties", resourceProperties,
            "PreviousResourceProperties", previousResourceProperties
        )
    );
}
}
```

Menerapkan base handler

1. Di IDE Anda, buka `BaseHookHandlerStd.java` file, yang terletak di `src/main/java/com/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `BaseHookHandlerStd.java` file dengan kode berikut.

Example Translator.java

```
package com.mycompany.testing.mytesthook;

import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.sqs.SqsClient;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.ProxyClient;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

public abstract class BaseHookHandlerStd extends BaseHookHandler<CallbackContext,
    TypeConfigurationModel> {
    public static final String HOOK_TYPE_NAME = "MyCompany::Testing::MyTestHook";

    protected Logger logger;

    @Override
    public ProgressEvent<HookTargetModel, CallbackContext> handleRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final Logger logger,
        final TypeConfigurationModel typeConfiguration
    ) {
        this.logger = logger;

        final String targetName = request.getHookContext().getTargetName();

        final ProgressEvent<HookTargetModel, CallbackContext> result;
        if (AwsS3Bucket.TYPE_NAME.equals(targetName)) {
```

```

        result = handleS3BucketRequest(
            proxy,
            request,
            callbackContext != null ? callbackContext : new
CallbackContext(),
            proxy.newProxy(ClientBuilder::createS3Client),
            typeConfiguration
        );
    } else if (AwsSqsQueue.TYPE_NAME.equals(targetName)) {
        result = handleSqsQueueRequest(
            proxy,
            request,
            callbackContext != null ? callbackContext : new
CallbackContext(),
            proxy.newProxy(ClientBuilder::createSqsClient),
            typeConfiguration
        );
    } else {
        throw new UnsupportedTargetException(targetName);
    }

    log(
        String.format(
            "Result for [%s] invocation for target [%s] returned status [%s]
with message [%s]",
            request.getHookContext().getInvocationPoint(),
            targetName,
            result.getStatus(),
            result.getMessage()
        )
    );

    return result;
}

protected abstract ProgressEvent<HookTargetModel, CallbackContext>
handleS3BucketRequest(
    final AmazonWebServicesClientProxy proxy,
    final HookHandlerRequest request,
    final CallbackContext callbackContext,
    final ProxyClient<S3Client> proxyClient,
    final TypeConfigurationModel typeConfiguration
);

```

```
protected abstract ProgressEvent<HookTargetModel, CallbackContext>
handleSqsQueueRequest(
    final AmazonWebServicesClientProxy proxy,
    final HookHandlerRequest request,
    final CallbackContext callbackContext,
    final ProxyClient<SqsClient> proxyClient,
    final TypeConfigurationModel typeConfiguration
);

protected void log(final String message) {
    if (logger != null) {
        logger.log(message);
    } else {
        System.out.println(message);
    }
}
}
```

Menerapkan **preCreate** handler

`preCreateHandler` memverifikasi pengaturan enkripsi sisi server untuk sumber daya atau sumber daya. `AWS::S3::Bucket` `AWS::SQS::Queue`

- Untuk `AWS::S3::Bucket` sumber daya, Hook hanya akan lulus jika berikut ini benar:
 - Enkripsi bucket Amazon S3 diatur.
 - Kunci bucket Amazon S3 diaktifkan untuk bucket.
 - Algoritma enkripsi yang ditetapkan untuk bucket Amazon S3 adalah algoritma yang benar yang diperlukan.
 - ID AWS Key Management Service kunci diatur.
- Untuk `AWS::SQS::Queue` sumber daya, Hook hanya akan lulus jika berikut ini benar:
 - ID AWS Key Management Service kunci diatur.

Mengkodekan **preCreate** handler

1. Di IDE Anda, buka `PreCreateHookHandler.java` file, yang terletak di `src/main/java/software/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `PreCreateHookHandler.java` file dengan kode berikut.

```
package com.mycompany.testing.mytesthook;

import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3BucketTargetModel;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.BucketEncryption;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionByDefault;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueueTargetModel;
import org.apache.commons.collections.CollectionUtils;
import org.apache.commons.lang3.StringUtils;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.hook.HookStatus;
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import
    software.amazon.cloudformation.proxy.hook.targetmodel.ResourceHookTargetModel;

import java.util.List;

public class PreCreateHookHandler extends BaseHookHandler<TypeConfigurationModel,
    CallbackContext> {

    @Override
    public HookProgressEvent<CallbackContext> handleRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final Logger logger,
        final TypeConfigurationModel typeConfiguration) {

        final String targetName = request.getHookContext().getTargetName();
        if ("AWS::S3::Bucket".equals(targetName)) {
            final ResourceHookTargetModel<AwsS3Bucket> targetModel =
                request.getHookContext().getTargetModel(AwsS3BucketTargetModel.class);

            final AwsS3Bucket bucket = targetModel.getResourceProperties();
```

```

        final String encryptionAlgorithm =
typeConfiguration.getEncryptionAlgorithm();

        return validateS3BucketEncryption(bucket, encryptionAlgorithm);

    } else if ("AWS::SQS::Queue".equals(targetName)) {
        final ResourceHookTargetModel<AwsSqsQueue> targetModel =
request.getHookContext().getTargetModel(AwsSqsQueueTargetModel.class);

        final AwsSqsQueue queue = targetModel.getResourceProperties();
        return validateSQSQueueEncryption(queue);
    } else {
        throw new UnsupportedTargetException(targetName);
    }
}

private HookProgressEvent<CallbackContext> validateS3BucketEncryption(final
AwsS3Bucket bucket, final String requiredEncryptionAlgorithm) {
    HookStatus resultStatus = null;
    String resultMessage = null;

    if (bucket != null) {
        final BucketEncryption bucketEncryption = bucket.getBucketEncryption();
        if (bucketEncryption != null) {
            final List<ServerSideEncryptionRule> serverSideEncryptionRules =
bucketEncryption.getServerSideEncryptionConfiguration();
            if (CollectionUtils.isNotEmpty(serverSideEncryptionRules)) {
                for (final ServerSideEncryptionRule rule :
serverSideEncryptionRules) {
                    final Boolean bucketKeyEnabled =
rule.getBucketKeyEnabled();
                    if (bucketKeyEnabled) {
                        final ServerSideEncryptionByDefault
serverSideEncryptionByDefault = rule.getServerSideEncryptionByDefault();

                        final String encryptionAlgorithm =
serverSideEncryptionByDefault.getSSEAlgorithm();
                        final String kmsKeyId =
serverSideEncryptionByDefault.getKMSMasterKeyID(); // "KMSMasterKeyID" is name of
the property for an AWS::S3::Bucket;

                        if (!StringUtils.equals(encryptionAlgorithm,
requiredEncryptionAlgorithm) && StringUtils.isBlank(kmsKeyId)) {
                            resultStatus = HookStatus.FAILED;

```

```

        resultMessage = "KMS Key ID not set
and SSE Encryption Algorithm is incorrect for bucket with name: " +
bucket.getBucketName();
        } else if (!StringUtils.equals(encryptionAlgorithm,
requiredEncryptionAlgorithm)) {
            resultStatus = HookStatus.FAILED;
            resultMessage = "SSE Encryption Algorithm is
incorrect for bucket with name: " + bucket.getBucketName();
        } else if (StringUtils.isBlank(kmsKeyId)) {
            resultStatus = HookStatus.FAILED;
            resultMessage = "KMS Key ID not set for bucket with
name: " + bucket.getBucketName();
        } else {
            resultStatus = HookStatus.SUCCESS;
            resultMessage = "Successfully invoked
PreCreateHookHandler for target: AWS::S3::Bucket";
        }
    } else {
        resultStatus = HookStatus.FAILED;
        resultMessage = "Bucket key not enabled for bucket with
name: " + bucket.getBucketName();
    }

    if (resultStatus == HookStatus.FAILED) {
        break;
    }
} else {
    resultStatus = HookStatus.FAILED;
    resultMessage = "No SSE Encryption configurations for bucket
with name: " + bucket.getBucketName();
}
} else {
    resultStatus = HookStatus.FAILED;
    resultMessage = "Bucket Encryption not enabled for bucket with
name: " + bucket.getBucketName();
}
} else {
    resultStatus = HookStatus.FAILED;
    resultMessage = "Resource properties for S3 Bucket target model are
empty";
}

return HookProgressEvent.<CallbackContext>builder()

```

```

        .status(resultStatus)
        .message(resultMessage)
        .errorCode(resultStatus == HookStatus.FAILED ?
HandlerErrorCode.ResourceConflict : null)
        .build();
    }

    private HookProgressEvent<CallbackContext> validateSQSQueueEncryption(final
AwsSqsQueue queue) {
        if (queue == null) {
            return HookProgressEvent.<CallbackContext>builder()
                .status(HookStatus.FAILED)
                .message("Resource properties for SQS Queue target model are
empty")
                .errorCode(HandlerErrorCode.ResourceConflict)
                .build();
        }

        final String kmsKeyId = queue.getKmsMasterKeyId(); // "KmsMasterKeyId" is
name of the property for an AWS::SQS::Queue
        if (StringUtils.isBlank(kmsKeyId)) {
            return HookProgressEvent.<CallbackContext>builder()
                .status(HookStatus.FAILED)
                .message("Server side encryption turned off for queue with
name: " + queue.getQueueName())
                .errorCode(HandlerErrorCode.ResourceConflict)
                .build();
        }

        return HookProgressEvent.<CallbackContext>builder()
            .status(HookStatus.SUCCESS)
            .message("Successfully invoked PreCreateHookHandler for target:
AWS::SQS::Queue")
            .build();
    }
}

```

Memperbarui **preCreate** tes

1. Di IDE Anda, buka `PreCreateHandlerTest.java` file, yang terletak di `src/test/java/software/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `PreCreateHandlerTest.java` file dengan kode berikut.

```
package com.mycompany.testing.mytesthook;

import com.google.common.collect.ImmutableMap;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.BucketEncryption;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionByDefault;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;
import org.junit.jupiter.api.BeforeEach;
import org.junit.jupiter.api.Test;
import org.junit.jupiter.api.extension.ExtendWith;
import org.mockito.Mock;
import org.mockito.junit.jupiter.MockitoExtension;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.hook.HookContext;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookStatus;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import java.util.Collections;
import java.util.Map;

import static org.assertj.core.api.Assertions.assertThat;
import static org.assertj.core.api.Assertions.assertThatExceptionOfType;
import static org.mockito.Mockito.mock;

@ExtendWith(MockitoExtension.class)
public class PreCreateHookHandlerTest {

    @Mock
    private AmazonWebServicesClientProxy proxy;

    @Mock
    private Logger logger;

    @BeforeEach
    public void setup() {
```

```
    proxy = mock(AmazonWebServicesClientProxy.class);
    logger = mock(Logger.class);
}

@Test
public void handleRequest_awsSqsQueueSuccess() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final AwsSqsQueue queue = buildSqsQueue("MyQueue", "KmsKey");
    final HookTargetModel targetModel = createHookTargetModel(queue);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::SQS::Queue").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.SUCCESS, "Successfully invoked
PreCreateHookHandler for target: AWS::SQS::Queue");
}

@Test
public void handleRequest_awsS3BucketSuccess() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", true,
"AES256", "KmsKey");
    final HookTargetModel targetModel = createHookTargetModel(bucket);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.SUCCESS, "Successfully invoked
PreCreateHookHandler for target: AWS::S3::Bucket");
}
```

```
@Test
public void handleRequest_awsS3BucketFail_bucketKeyNotEnabled() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", false,
"AES256", "KmsKey");
    final HookTargetModel targetModel = createHookTargetModel(bucket);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.FAILED, "Bucket key not enabled for
bucket with name: amzn-s3-demo-bucket");
}

@Test
public void handleRequest_awsS3BucketFail_incorrectSSEEncryptionAlgorithm() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", true,
"SHA512", "KmsKey");
    final HookTargetModel targetModel = createHookTargetModel(bucket);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.FAILED, "SSE Encryption Algorithm is
incorrect for bucket with name: amzn-s3-demo-bucket");
}

@Test
```

```
public void handleRequest_awsS3BucketFail_kmsKeyIdNotSet() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final AwsS3Bucket bucket = buildAwsS3Bucket("amzn-s3-demo-bucket", true,
"AES256", null);
    final HookTargetModel targetModel = createHookTargetModel(bucket);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.FAILED, "KMS Key ID not set for bucket
with name: amzn-s3-demo-bucket");
}

@Test
public void handleRequest_awsSqsQueueFail_serverSideEncryptionOff() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();

    final AwsSqsQueue queue = buildSqsQueue("MyQueue", null);
    final HookTargetModel targetModel = createHookTargetModel(queue);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::SQS::Queue").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.FAILED, "Server side encryption turned
off for queue with name: MyQueue");
}

@Test
public void handleRequest_unsupportedTarget() {
    final PreCreateHookHandler handler = new PreCreateHookHandler();
```

```

        final Map<String, Object> unsupportedTarget =
ImmutableMap.of("ResourceName", "MyUnsupportedTarget");
        final HookTargetModel targetModel =
createHookTargetModel(unsupportedTarget);
        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::Unsupported::Target").targetModel(targetModel)
        .build());

        assertThatExceptionOfType(UnsupportedTargetException.class)
            .isThrownBy(() -> handler.handleRequest(proxy, request, null,
logger, typeConfiguration))
            .withMessageContaining("Unsupported target")
            .withMessageContaining("AWS::Unsupported::Target")
            .satisfies(e ->
assertThat(e.getErrorCode()).isEqualTo(HandlerErrorCode.InvalidRequest));
    }

    private void assertResponse(final HookProgressEvent<CallbackContext> response,
final HookStatus expectedStatus, final String expectedErrorMsg) {
        assertThat(response).isNotNull();
        assertThat(response.getStatus()).isEqualTo(expectedStatus);
        assertThat(response.getCallbackContext()).isNull();
        assertThat(response.getCallbackDelaySeconds()).isEqualTo(0);
        assertThat(response.getMessage()).isNotNull();
        assertThat(response.getMessage()).isEqualTo(expectedErrorMsg);
    }

    private HookTargetModel createHookTargetModel(final Object resourceProperties)
{
        return HookTargetModel.of(ImmutableMap.of("ResourceProperties",
resourceProperties));
    }

    @SuppressWarnings("SameParameterValue")
    private AwsSqsQueue buildSqsQueue(final String queueName, final String
kmsKeyId) {
        return AwsSqsQueue.builder()
            .queueName(queueName)
            .kmsMasterKeyId(kmsKeyId) // "KmsMasterKeyId" is name of the
property for an AWS::SQS::Queue

```

```

        .build();
    }

    @SuppressWarnings("SameParameterValue")
    private AwsS3Bucket buildAwsS3Bucket(
        final String bucketName,
        final Boolean bucketKeyEnabled,
        final String sseAlgorithm,
        final String kmsKeyId
    ) {
        return AwsS3Bucket.builder()
            .bucketName(bucketName)
            .bucketEncryption(
                BucketEncryption.builder()
                    .serverSideEncryptionConfiguration(
                        Collections.singletonList(
                            ServerSideEncryptionRule.builder()
                                .bucketKeyEnabled(bucketKeyEnabled)
                                .serverSideEncryptionByDefault(
                                    ServerSideEncryptionByDefault.builder()
                                        .sSEAlgorithm(sseAlgorithm)
                                        .kMSMasterKeyID(kmsKeyId) //
                                        .build()
                                )
                            ).build()
                        )
                    ).build()
            ).build();
    }
}

```

"KMSMasterKeyID" is name of the property for an AWS::S3::Bucket

Menerapkan **preUpdate** handler

Menerapkan `preUpdate` handler, yang memulai sebelum operasi update untuk semua target yang ditentukan dalam handler. `preUpdateHandler` menyelesaikan hal berikut:

- Untuk `AWS::S3::Bucket` sumber daya, Hook hanya akan lulus jika berikut ini benar:
 - Algoritma enkripsi bucket untuk bucket Amazon S3 belum dimodifikasi.

Mengkodekan **preUpdate** handler

1. Di IDE Anda, buka `PreUpdateHookHandler.java` file, yang terletak di `src/main/java/software/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `PreUpdateHookHandler.java` file dengan kode berikut.

```
package com.mycompany.testing.mytesthook;

import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3BucketTargetModel;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;
import org.apache.commons.lang3.StringUtils;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.hook.HookStatus;
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import
    software.amazon.cloudformation.proxy.hook.targetmodel.ResourceHookTargetModel;

import java.util.List;

public class PreUpdateHookHandler extends BaseHookHandler<TypeConfigurationModel,
    CallbackContext> {

    @Override
    public HookProgressEvent<CallbackContext> handleRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final Logger logger,
        final TypeConfigurationModel typeConfiguration) {

        final String targetName = request.getHookContext().getTargetName();
        if ("AWS::S3::Bucket".equals(targetName)) {
            final ResourceHookTargetModel<AwsS3Bucket> targetModel =
                request.getHookContext().getTargetModel(AwsS3BucketTargetModel.class);

            final AwsS3Bucket bucketProperties =
                targetModel.getResourceProperties();
```

```

        final AwsS3Bucket previousBucketProperties =
targetModel.getPreviousResourceProperties();

        return validateBucketEncryptionRulesNotUpdated(bucketProperties,
previousBucketProperties);
    } else {
        throw new UnsupportedTargetException(targetName);
    }
}

private HookProgressEvent<CallbackContext>
validateBucketEncryptionRulesNotUpdated(final AwsS3Bucket resourceProperties,
final AwsS3Bucket previousResourceProperties) {
    final List<ServerSideEncryptionRule> bucketEncryptionConfigs =
resourceProperties.getBucketEncryption().getServerSideEncryptionConfiguration();
    final List<ServerSideEncryptionRule> previousBucketEncryptionConfigs =
previousResourceProperties.getBucketEncryption().getServerSideEncryptionConfiguration();

    if (bucketEncryptionConfigs.size() !=
previousBucketEncryptionConfigs.size()) {
        return HookProgressEvent.<CallbackContext>builder()
            .status(HookStatus.FAILED)
            .errorCode(HandlerErrorCode.NotUpdatable)
            .message(
                String.format(
                    "Current number of bucket encryption configs does not
match previous. Current has %d configs while previously there were %d configs",
                    bucketEncryptionConfigs.size(),
                    previousBucketEncryptionConfigs.size()
                )
            ).build();
    }

    for (int i = 0; i < bucketEncryptionConfigs.size(); ++i) {
        final String currentEncryptionAlgorithm =
bucketEncryptionConfigs.get(i).getServerSideEncryptionByDefault().getSSEAlgorithm();
        final String previousEncryptionAlgorithm =
previousBucketEncryptionConfigs.get(i).getServerSideEncryptionByDefault().getSSEAlgorithm();

        if (!StringUtils.equals(currentEncryptionAlgorithm,
previousEncryptionAlgorithm)) {
            return HookProgressEvent.<CallbackContext>builder()
                .status(HookStatus.FAILED)
                .errorCode(HandlerErrorCode.NotUpdatable)

```

```

        .message(
            String.format(
                "Bucket Encryption algorithm can not be changed once
set. The encryption algorithm was changed to '%s' from '%s'.",
                currentEncryptionAlgorithm,
                previousEncryptionAlgorithm
            )
        )
        .build();
    }
}

return HookProgressEvent.<CallbackContext>builder()
    .status(HookStatus.SUCCESS)
    .message("Successfully invoked PreUpdateHookHandler for target:
AWS::SQS::Queue")
    .build();
}
}

```

Memperbarui **preUpdate** tes

1. Di IDE Anda, buka `PreUpdateHandlerTest.java` file di `src/main/java/com/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `PreUpdateHandlerTest.java` file dengan kode berikut.

```

package com.mycompany.testing.mytesthook;

import com.google.common.collect.ImmutableMap;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.BucketEncryption;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionByDefault;
import
    com.mycompany.testing.mytesthook.model.aws.s3.bucket.ServerSideEncryptionRule;
import org.junit.jupiter.api.BeforeEach;
import org.junit.jupiter.api.Test;
import org.junit.jupiter.api.extension.ExtendWith;
import org.mockito.Mock;
import org.mockito.junit.jupiter.MockitoExtension;
import software.amazon.cloudformation.exceptions.UnsupportedTargetException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;

```

```
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.hook.HookContext;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.HookProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookStatus;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import java.util.Arrays;
import java.util.stream.Stream;

import static org.assertj.core.api.Assertions.assertThat;
import static org.assertj.core.api.Assertions.assertThatExceptionOfType;
import static org.mockito.Mockito.mock;

@ExtendWith(MockitoExtension.class)
public class PreUpdateHookHandlerTest {

    @Mock
    private AmazonWebServicesClientProxy proxy;

    @Mock
    private Logger logger;

    @BeforeEach
    public void setup() {
        proxy = mock(AmazonWebServicesClientProxy.class);
        logger = mock(Logger.class);
    }

    @Test
    public void handleRequest_awsS3BucketSuccess() {
        final PreUpdateHookHandler handler = new PreUpdateHookHandler();

        final ServerSideEncryptionRule serverSideEncryptionRule =
            buildServerSideEncryptionRule("AES256");
        final AwsS3Bucket resourceProperties = buildAwsS3Bucket("amzn-s3-demo-
            bucket", serverSideEncryptionRule);
        final AwsS3Bucket previousResourceProperties = buildAwsS3Bucket("amzn-s3-
            demo-bucket", serverSideEncryptionRule);
        final HookTargetModel targetModel =
            createHookTargetModel(resourceProperties, previousResourceProperties);
        final TypeConfigurationModel typeConfiguration =
            TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();
```

```
        final HookHandlerRequest request = HookHandlerRequest.builder()

        .hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
            .build());

        final HookProgressEvent<CallbackContext> response =
        handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.SUCCESS, "Successfully invoked
        PreUpdateHookHandler for target: AWS::SQS::Queue");
    }

    @Test
    public void handleRequest_awsS3BucketFail_bucketEncryptionConfigsDontMatch() {
        final PreUpdateHookHandler handler = new PreUpdateHookHandler();

        final ServerSideEncryptionRule[] serverSideEncryptionRules =
        Stream.of("AES256", "SHA512", "AES32")
            .map(this::buildServerSideEncryptionRule)
            .toArray(ServerSideEncryptionRule[]::new);

        final AwsS3Bucket resourceProperties = buildAwsS3Bucket("amzn-s3-demo-
        bucket", serverSideEncryptionRules[0]);
        final AwsS3Bucket previousResourceProperties = buildAwsS3Bucket("amzn-s3-
        demo-bucket", serverSideEncryptionRules);
        final HookTargetModel targetModel =
        createHookTargetModel(resourceProperties, previousResourceProperties);
        final TypeConfigurationModel typeConfiguration =
        TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

        final HookHandlerRequest request = HookHandlerRequest.builder()

        .hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
            .build());

        final HookProgressEvent<CallbackContext> response =
        handler.handleRequest(proxy, request, null, logger, typeConfiguration);
        assertResponse(response, HookStatus.FAILED, "Current number of bucket
        encryption configs does not match previous. Current has 1 configs while previously
        there were 3 configs");
    }

    @Test
```

```

public void
handleRequest_awsS3BucketFail_bucketEncryptionAlgorithmDoesNotMatch() {
    final PreUpdateHookHandler handler = new PreUpdateHookHandler();

    final AwsS3Bucket resourceProperties = buildAwsS3Bucket("amzn-s3-demo-
bucket", buildServerSideEncryptionRule("SHA512"));
    final AwsS3Bucket previousResourceProperties = buildAwsS3Bucket("amzn-s3-
demo-bucket", buildServerSideEncryptionRule("AES256"));
    final HookTargetModel targetModel =
createHookTargetModel(resourceProperties, previousResourceProperties);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::S3::Bucket").targetModel(targetModel)
    .build());

    final HookProgressEvent<CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);
    assertResponse(response, HookStatus.FAILED, String.format("Bucket
Encryption algorithm can not be changed once set. The encryption algorithm was
changed to '%s' from '%s'.", "SHA512", "AES256"));
}

@Test
public void handleRequest_unsupportedTarget() {
    final PreUpdateHookHandler handler = new PreUpdateHookHandler();

    final Object resourceProperties = ImmutableMap.of("FileSizeLimit", 256);
    final Object previousResourceProperties = ImmutableMap.of("FileSizeLimit",
512);
    final HookTargetModel targetModel =
createHookTargetModel(resourceProperties, previousResourceProperties);
    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder().encryptionAlgorithm("AES256").build();

    final HookHandlerRequest request = HookHandlerRequest.builder()

.hookContext(HookContext.builder().targetName("AWS::Unsupported::Target").targetModel(targ
    .build());

    assertThatExceptionOfType(UnsupportedTargetException.class)

```

```
        .isThrownBy(() -> handler.handleRequest(proxy, request, null,
logger, typeConfiguration))
        .withMessageContaining("Unsupported target")
        .withMessageContaining("AWS::Unsupported::Target")
        .satisfies(e ->
assertThat(e.getErrorCode()).isEqualTo(HandlerErrorCode.InvalidRequest));
    }

    private void assertResponse(final HookProgressEvent<CallbackContext> response,
final HookStatus expectedStatus, final String expectedErrorMsg) {
        assertThat(response).isNotNull();
        assertThat(response.getStatus()).isEqualTo(expectedStatus);
        assertThat(response.getCallbackContext()).isNull();
        assertThat(response.getCallbackDelaySeconds()).isEqualTo(0);
        assertThat(response.getMessage()).isNotNull();
        assertThat(response.getMessage()).isEqualTo(expectedErrorMsg);
    }

    private HookTargetModel createHookTargetModel(final Object resourceProperties,
final Object previousResourceProperties) {
        return HookTargetModel.of(
            ImmutableMap.of(
                "ResourceProperties", resourceProperties,
                "PreviousResourceProperties", previousResourceProperties
            )
        );
    }

    @SuppressWarnings("SameParameterValue")
    private AwsS3Bucket buildAwsS3Bucket(
        final String bucketName,
        final ServerSideEncryptionRule ...serverSideEncryptionRules
    ) {
        return AwsS3Bucket.builder()
            .bucketName(bucketName)
            .bucketEncryption(
                BucketEncryption.builder()
                    .serverSideEncryptionConfiguration(
                        Arrays.asList(serverSideEncryptionRules)
                    ).build()
            ).build();
    }
}
```

```

private ServerSideEncryptionRule buildServerSideEncryptionRule(final String
encryptionAlgorithm) {
    return ServerSideEncryptionRule.builder()
        .bucketKeyEnabled(true)
        .serverSideEncryptionByDefault(
            ServerSideEncryptionByDefault.builder()
                .sSEAlgorithm(encryptionAlgorithm)
                .build()
        ).build();
}
}

```

Menerapkan **preDelete** handler

Menerapkan **preDelete** handler, yang memulai sebelum operasi penghapusan untuk semua target yang ditentukan dalam handler. **preDeleteHandler** menyelesaikan hal berikut:

- Untuk `AWS::S3::Bucket` sumber daya, Hook hanya akan lulus jika berikut ini benar:
 - Memverifikasi bahwa sumber daya keluhan minimum yang diperlukan akan ada di akun setelah menghapus sumber daya.
 - Jumlah sumber daya keluhan minimum yang diperlukan ditetapkan dalam konfigurasi tipe Hook.

Mengkodekan **preDelete** handler

1. Di IDE Anda, buka `PreDeleteHookHandler.java` file di `src/main/java/com/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `PreDeleteHookHandler.java` file dengan kode berikut.

```

package com.mycompany.testing.mytesthook;

import com.google.common.annotations.VisibleForTesting;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3BucketTargetModel;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueue;
import com.mycompany.testing.mytesthook.model.aws.sqs.queue.AwsSqsQueueTargetModel;
import org.apache.commons.lang3.StringUtils;
import org.apache.commons.lang3.math.NumberUtils;
import software.amazon.awssdk.services.cloudformation.CloudFormationClient;
import
    software.amazon.awssdk.services.cloudformation.model.CloudFormationException;

```

```
import
    software.amazon.awssdk.services.cloudformation.model.DescribeStackResourceRequest;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.sqs.SqsClient;
import software.amazon.awssdk.services.sqs.model.GetQueueAttributesRequest;
import software.amazon.awssdk.services.sqs.model.GetQueueUrlRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesResponse;
import software.amazon.awssdk.services.sqs.model.QueueAttributeName;
import software.amazon.awssdk.services.sqs.model.SqsException;
import software.amazon.cloudformation.exceptions.CfnGeneralServiceException;
import software.amazon.cloudformation.proxy.AmazonWebServicesClientProxy;
import software.amazon.cloudformation.proxy.HandlerErrorCode;
import software.amazon.cloudformation.proxy.OperationStatus;
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.ProxyClient;
import software.amazon.cloudformation.proxy.hook.HookContext;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;
import
    software.amazon.cloudformation.proxy.hook.targetmodel.ResourceHookTargetModel;

import java.util.ArrayList;
import java.util.Collection;
import java.util.HashSet;
import java.util.List;
import java.util.Objects;
import java.util.stream.Collectors;

public class PreDeleteHookHandler extends BaseHookHandlerStd {

    private ProxyClient<S3Client> s3Client;
    private ProxyClient<SqsClient> sqsClient;

    @Override
    protected ProgressEvent<HookTargetModel, CallbackContext>
    handleS3BucketRequest(
        final AmazonWebServicesClientProxy proxy,
        final HookHandlerRequest request,
        final CallbackContext callbackContext,
        final ProxyClient<S3Client> proxyClient,
        final TypeConfigurationModel typeConfiguration
```

```
) {
    final HookContext hookContext = request.getHookContext();
    final String targetName = hookContext.getTargetName();
    if (!AwsS3Bucket.TYPE_NAME.equals(targetName)) {
        throw new RuntimeException(String.format("Request target type [%s] is
not 'AWS::S3::Bucket'", targetName));
    }
    this.s3Client = proxyClient;

    final String encryptionAlgorithm =
typeConfiguration.getEncryptionAlgorithm();
    final int minBuckets =
NumberUtils.toInt(typeConfiguration.getMinBuckets());

    final ResourceHookTargetModel<AwsS3Bucket> targetModel =
hookContext.getTargetModel(AwsS3BucketTargetModel.class);
    final List<String> buckets = listBuckets().stream()
        .filter(b -> !StringUtils.equals(b,
targetModel.getResourceProperties().getBucketName()))
        .collect(Collectors.toList());

    final List<String> compliantBuckets = new ArrayList<>();
    for (final String bucket : buckets) {
        if (getBucketSSEAlgorithm(bucket).contains(encryptionAlgorithm)) {
            compliantBuckets.add(bucket);
        }

        if (compliantBuckets.size() >= minBuckets) {
            return ProgressEvent.<HookTargetModel, CallbackContext>builder()
                .status(OperationStatus.SUCCESS)
                .message("Successfully invoked PreDeleteHookHandler for
target: AWS::S3::Bucket")
                .build();
        }
    }

    return ProgressEvent.<HookTargetModel, CallbackContext>builder()
        .status(OperationStatus.FAILED)
        .errorCode(HandlerErrorCode.NonCompliant)
        .message(String.format("Failed to meet minimum of [%d] encrypted
buckets.", minBuckets))
        .build();
}
```

```

@Override
protected ProgressEvent<HookTargetModel, CallbackContext>
handleSqsQueueRequest(
    final AmazonWebServicesClientProxy proxy,
    final HookHandlerRequest request,
    final CallbackContext callbackContext,
    final ProxyClient<SqsClient> proxyClient,
    final TypeConfigurationModel typeConfiguration
) {
    final HookContext hookContext = request.getHookContext();
    final String targetName = hookContext.getTargetName();
    if (!AwsSqsQueue.TYPE_NAME.equals(targetName)) {
        throw new RuntimeException(String.format("Request target type [%s] is
not 'AWS::SQS::Queue'", targetName));
    }
    this.sqsClient = proxyClient;
    final int minQueues = NumberUtils.toInt(typeConfiguration.getMinQueues());

    final ResourceHookTargetModel<AwsSqsQueue> targetModel =
hookContext.getTargetModel(AwsSqsQueueTargetModel.class);

    final String queueName =
Objects.toString(targetModel.getResourceProperties().get("QueueName"), null);

    String targetQueueUrl = null;
    if (queueName != null) {
        try {
            targetQueueUrl = sqsClient.injectCredentialsAndInvokeV2(
                GetQueueUrlRequest.builder().queueName(
                    queueName
                ).build(),
                sqsClient.client()::getQueueUrl
            ).queueUrl();
        } catch (SqsException e) {
            log(String.format("Error while calling GetQueueUrl API for queue
name [%s]: %s", queueName, e.getMessage()));
        }
    } else {
        log("Queue name is empty, attempting to get queue's physical ID");
        try {
            final ProxyClient<CloudFormationClient> cfnClient =
proxy.newProxy(ClientBuilder::createCloudFormationClient);
            targetQueueUrl = cfnClient.injectCredentialsAndInvokeV2(
                DescribeStackResourceRequest.builder()

```

```

        .stackName(hookContext.getTargetLogicalId())

.logicalResourceId(hookContext.getTargetLogicalId())
        .build(),
        cfnClient.client()::describeStackResource
    ).stackResourceDetail().physicalResourceId();
    } catch (CloudFormationException e) {
        log(String.format("Error while calling DescribeStackResource API
for queue name: %s", e.getMessage()));
    }
}

// Creating final variable for the filter lambda
final String finalTargetQueueUrl = targetQueueUrl;

final List<String> compliantQueues = new ArrayList<>();

String nextToken = null;
do {
    final ListQueuesRequest req =
Translator.createListQueuesRequest(nextToken);
    final ListQueuesResponse res =
sqsClient.injectCredentialsAndInvokeV2(req, sqsClient.client()::listQueues);
    final List<String> queueUrls = res.queueUrls().stream()
        .filter(q -> !StringUtils.equals(q, finalTargetQueueUrl))
        .collect(Collectors.toList());

    for (final String queueUrl : queueUrls) {
        if (isQueueEncrypted(queueUrl)) {
            compliantQueues.add(queueUrl);
        }

        if (compliantQueues.size() >= minQueues) {
            return ProgressEvent.<HookTargetModel,
CallbackContext>builder()
                .status(OperationStatus.SUCCESS)
                .message("Successfully invoked PreDeleteHookHandler for
target: AWS::SQS::Queue")
                .build();
        }
        nextToken = res.nextToken();
    }
} while (nextToken != null);

```

```
        return ProgressEvent.<HookTargetModel, CallbackContext>builder()
            .status(OperationStatus.FAILED)
            .errorCode(HandlerErrorCode.NonCompliant)
            .message(String.format("Failed to meet minimum of [%d] encrypted
queues.", minQueues))
            .build();
    }

    private List<String> listBuckets() {
        try {
            return
s3Client.injectCredentialsAndInvokeV2(Translator.createListBucketsRequest(),
s3Client.client()::listBuckets)
                .buckets()
                .stream()
                .map(Bucket::name)
                .collect(Collectors.toList());
        } catch (S3Exception e) {
            throw new CfnGeneralServiceException("Error while calling S3
ListBuckets API", e);
        }
    }

    @VisibleForTesting
    Collection<String> getBucketSSEAlgorithm(final String bucket) {
        try {
            return
s3Client.injectCredentialsAndInvokeV2(Translator.createGetBucketEncryptionRequest(bucket),
s3Client.client()::getBucketEncryption)
                .serverSideEncryptionConfiguration()
                .rules()
                .stream()
                .filter(r ->
Objects.nonNull(r.applyServerSideEncryptionByDefault()))
                .map(r ->
r.applyServerSideEncryptionByDefault().sseAlgorithmAsString())
                .collect(Collectors.toSet());
        } catch (S3Exception e) {
            return new HashSet<>();
        }
    }

    @VisibleForTesting
    boolean isQueueEncrypted(final String queueUrl) {
```

```
    try {
        final GetQueueAttributesRequest request =
            GetQueueAttributesRequest.builder()
                .queueUrl(queueUrl)
                .attributeNames(QueueAttributeName.KMS_MASTER_KEY_ID)
                .build();
        final String kmsKeyId = sqsClient.injectCredentialsAndInvokeV2(request,
            sqsClient.client()::getQueueAttributes)
            .attributes()
            .get(QueueAttributeName.KMS_MASTER_KEY_ID);

        return StringUtils.isNotBlank(kmsKeyId);
    } catch (SqsException e) {
        throw new CfnGeneralServiceException("Error while calling SQS
            GetQueueAttributes API", e);
    }
}
```

Memperbarui **preDelete** handler

1. Di IDE Anda, buka `PreDeleteHookHandler.java` file di `src/main/java/com/mycompany/testing/mytesthook` folder.
2. Ganti seluruh isi `PreDeleteHookHandler.java` file dengan kode berikut.

```
package com.mycompany.testing.mytesthook;

import com.google.common.collect.ImmutableList;
import com.google.common.collect.ImmutableMap;
import com.mycompany.testing.mytesthook.model.aws.s3.bucket.AwsS3Bucket;
import org.junit.jupiter.api.BeforeEach;
import org.junit.jupiter.api.Test;
import org.junit.jupiter.api.extension.ExtendWith;
import org.mockito.Mock;
import org.mockito.Mockito;
import org.mockito.junit.jupiter.MockitoExtension;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.GetBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.GetBucketEncryptionResponse;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsResponse;
```

```
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionByDefault;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionConfiguration;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionRule;
import software.amazon.awssdk.services.sqs.SqsClient;
import software.amazon.awssdk.services.sqs.model.GetQueueAttributesRequest;
import software.amazon.awssdk.services.sqs.model.GetQueueAttributesResponse;
import software.amazon.awssdk.services.sqs.model.GetQueueUrlRequest;
import software.amazon.awssdk.services.sqs.model.GetQueueUrlResponse;
import software.amazon.awssdk.services.sqs.model.ListQueuesRequest;
import software.amazon.awssdk.services.sqs.model.ListQueuesResponse;
import software.amazon.awssdk.services.sqs.model.QueueAttributeName;
import software.amazon.cloudformation.proxy.Logger;
import software.amazon.cloudformation.proxy.OperationStatus;
import software.amazon.cloudformation.proxy.ProgressEvent;
import software.amazon.cloudformation.proxy.hook.HookContext;
import software.amazon.cloudformation.proxy.hook.HookHandlerRequest;
import software.amazon.cloudformation.proxy.hook.targetmodel.HookTargetModel;

import java.util.Arrays;
import java.util.Collection;
import java.util.HashMap;
import java.util.List;
import java.util.stream.Collectors;

import static org.mockito.ArgumentMatchers.any;
import static org.mockito.Mockito.mock;
import static org.mockito.Mockito.never;
import static org.mockito.Mockito.times;
import static org.mockito.Mockito.verify;
import static org.mockito.Mockito.when;

@ExtendWith(MockitoExtension.class)
public class PreDeleteHookHandlerTest extends AbstractTestBase {

    @Mock private S3Client s3Client;
    @Mock private SqsClient sqsClient;
    @Mock private Logger logger;

    @BeforeEach
    public void setup() {
        s3Client = mock(S3Client.class);
        sqsClient = mock(SqsClient.class);
        logger = mock(Logger.class);
    }
}
```

```
}

@Test
public void handleRequest_awsS3BucketSuccess() {
    final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

    final List<Bucket> bucketList = ImmutableList.of(
        Bucket.builder().name("bucket1").build(),
        Bucket.builder().name("bucket2").build(),
        Bucket.builder().name("toBeDeletedBucket").build(),
        Bucket.builder().name("bucket3").build(),
        Bucket.builder().name("bucket4").build(),
        Bucket.builder().name("bucket5").build()
    );
    final ListBucketsResponse mockResponse =
ListBucketsResponse.builder().buckets(bucketList).build();

when(s3Client.listBuckets(any(ListBucketsRequest.class))).thenReturn(mockResponse);
when(s3Client.getBucketEncryption(any(GetBucketEncryptionRequest.class)))
    .thenReturn(buildGetBucketEncryptionResponse("AES256"))
    .thenReturn(buildGetBucketEncryptionResponse("AES256", "aws:kms"))
    .thenThrow(S3Exception.builder().message("No Encrypt").build())
    .thenReturn(buildGetBucketEncryptionResponse("aws:kms"))
    .thenReturn(buildGetBucketEncryptionResponse("AES256"));
setServiceClient(s3Client);

    final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
        .encryptionAlgorithm("AES256")
        .minBuckets("3")
        .build();

    final HookHandlerRequest request = HookHandlerRequest.builder()
        .hookContext(
            HookContext.builder()
                .targetName("AWS::S3::Bucket")
                .targetModel(
                    createHookTargetModel(
                        AwsS3Bucket.builder()
                            .bucketName("toBeDeletedBucket")
                            .build()
                    )
                )
        )
    )
}
```

```

        .build())
        .build();

        final ProgressEvent<HookTargetModel, CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);

        verify(s3Client,
times(5)).getBucketEncryption(any(GetBucketEncryptionRequest.class));
        verify(handler, never()).getBucketSSEAlgorithm("toBeDeletedBucket");

        assertResponse(response, OperationStatus.SUCCESS, "Successfully invoked
PreDeleteHookHandler for target: AWS::S3::Bucket");
    }

@Test
public void handleRequest_awsSqsQueueSuccess() {
    final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

    final List<String> queueUrls = ImmutableList.of(
        "https://queue1.queue",
        "https://queue2.queue",
        "https://toBeDeletedQueue.queue",
        "https://queue3.queue",
        "https://queue4.queue",
        "https://queue5.queue"
    );

    when(sqsClient.getQueueUrl(any(GetQueueUrlRequest.class)))
        .thenReturn(GetQueueUrlResponse.builder().queueUrl("https://
toBeDeletedQueue.queue").build());
    when(sqsClient.listQueues(any(ListQueuesRequest.class)))

.thenReturn(ListQueuesResponse.builder().queueUrls(queueUrls).build());
        when(sqsClient.getQueueAttributes(any(GetQueueAttributesRequest.class)))

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())
            .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())

.thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())

```

```

        .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())

        .thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttributes
"kmsKeyId")).build());
        setServiceClient(sqsClient);

        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
        .minQueues("3")
        .build();

        final HookHandlerRequest request = HookHandlerRequest.builder()
        .hookContext(
            HookContext.builder()
            .targetName("AWS::SQS::Queue")
            .targetModel(
                createHookTargetModel(
                    ImmutableMap.of("QueueName", "toBeDeletedQueue")
                )
            )
            .build())
        .build();

        final ProgressEvent<HookTargetModel, CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);

        verify(sqsClient,
times(5)).getQueueAttributes(any(GetQueueAttributesRequest.class));
        verify(handler, never()).isQueueEncrypted("toBeDeletedQueue");

        assertResponse(response, OperationStatus.SUCCESS, "Successfully invoked
PreDeleteHookHandler for target: AWS::SQS::Queue");
    }

    @Test
    public void handleRequest_awsS3BucketFailed() {
        final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

        final List<Bucket> bucketList = ImmutableList.of(
            Bucket.builder().name("bucket1").build(),
            Bucket.builder().name("bucket2").build(),
            Bucket.builder().name("toBeDeletedBucket").build(),

```

```
        Bucket.builder().name("bucket3").build(),
        Bucket.builder().name("bucket4").build(),
        Bucket.builder().name("bucket5").build()
    );
    final ListBucketsResponse mockResponse =
ListBucketsResponse.builder().buckets(bucketList).build();

when(s3Client.listBuckets(any(ListBucketsRequest.class))).thenReturn(mockResponse);
when(s3Client.getBucketEncryption(any(GetBucketEncryptionRequest.class)))
    .thenReturn(buildGetBucketEncryptionResponse("AES256"))
    .thenReturn(buildGetBucketEncryptionResponse("AES256", "aws:kms"))
    .thenThrow(S3Exception.builder().message("No Encrypt").build())
    .thenReturn(buildGetBucketEncryptionResponse("aws:kms"))
    .thenReturn(buildGetBucketEncryptionResponse("AES256"));
setServiceClient(s3Client);

final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
    .encryptionAlgorithm("AES256")
    .minBuckets("10")
    .build();

final HookHandlerRequest request = HookHandlerRequest.builder()
    .hookContext(
        HookContext.builder()
            .targetName("AWS::S3::Bucket")
            .targetModel(
                createHookTargetModel(
                    AwsS3Bucket.builder()
                        .bucketName("toBeDeletedBucket")
                        .build()
                )
            )
            .build()
    )
    .build();

final ProgressEvent<HookTargetModel, CallbackContext> response =
handler.handleRequest(proxy, request, null, logger, typeConfiguration);

verify(s3Client,
times(5)).getBucketEncryption(any(GetBucketEncryptionRequest.class));
verify(handler, never()).getBucketSSEAlgorithm("toBeDeletedBucket");
```

```

        assertResponse(response, OperationStatus.FAILED, "Failed to meet minimum of
[10] encrypted buckets.");
    }

    @Test
    public void handleRequest_awsSqsQueueFailed() {
        final PreDeleteHookHandler handler = Mockito.spy(new
PreDeleteHookHandler());

        final List<String> queueUrls = ImmutableList.of(
            "https://queue1.queue",
            "https://queue2.queue",
            "https://toBeDeletedQueue.queue",
            "https://queue3.queue",
            "https://queue4.queue",
            "https://queue5.queue"
        );

        when(sqsClient.getQueueUrl(any(GetQueueUrlRequest.class)))
            .thenReturn(GetQueueUrlResponse.builder().queueUrl("https://
toBeDeletedQueue.queue").build());
        when(sqsClient.listQueues(any(ListQueuesRequest.class)))
            .thenReturn(ListQueuesResponse.builder().queueUrls(queueUrls).build());
        when(sqsClient.getQueueAttributes(any(GetQueueAttributesRequest.class)))
            .thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())
            .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())
            .thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build())
            .thenReturn(GetQueueAttributesResponse.builder().attributes(new
HashMap<>()).build())
            .thenReturn(GetQueueAttributesResponse.builder().attributes(ImmutableMap.of(QueueAttribute
"kmsKeyId")).build());
        setServiceClient(sqsClient);

        final TypeConfigurationModel typeConfiguration =
TypeConfigurationModel.builder()
            .minQueues("10")

```

```

        .build();

    final HookHandlerRequest request = HookHandlerRequest.builder()
        .hookContext(
            HookContext.builder()
                .targetName("AWS::SQS::Queue")
                .targetModel(
                    createHookTargetModel(
                        ImmutableMap.of("QueueName", "toBeDeletedQueue")
                    )
                )
                .build()
            )
        .build();

    final ProgressEvent<HookTargetModel, CallbackContext> response =
    handler.handleRequest(proxy, request, null, logger, typeConfiguration);

    verify(sqsClient,
    times(5)).getQueueAttributes(any(GetQueueAttributesRequest.class));
    verify(handler, never()).isQueueEncrypted("toBeDeletedQueue");

    assertResponse(response, OperationStatus.FAILED, "Failed to meet minimum of
    [10] encrypted queues.");
}

private GetBucketEncryptionResponse buildGetBucketEncryptionResponse(final
String ...sseAlgorithm) {
    return buildGetBucketEncryptionResponse(
        Arrays.stream(sseAlgorithm)
            .map(a ->
                ServerSideEncryptionRule.builder().applyServerSideEncryptionByDefault(
                    ServerSideEncryptionByDefault.builder()
                        .sseAlgorithm(a)
                        .build()
                ).build()
            )
        ).collect(Collectors.toList())
    );
}

private GetBucketEncryptionResponse buildGetBucketEncryptionResponse(final
Collection<ServerSideEncryptionRule> rules) {
    return GetBucketEncryptionResponse.builder()
        .serverSideEncryptionConfiguration(

```

```
        ServerSideEncryptionConfiguration.builder().rules(  
            rules  
        ).build()  
    ).build();  
}  
}
```

Pemodelan CloudFormation Hooks kustom menggunakan Python

Pemodelan CloudFormation Hooks kustom melibatkan pembuatan skema yang mendefinisikan Hook, propertinya, dan atributnya. Tutorial ini memandu Anda melalui pemodelan Hooks kustom menggunakan Python.

Langkah 1: Buat paket proyek Hook

Hasilkan paket proyek Hook Anda. CloudFormation CLI menciptakan fungsi handler kosong yang sesuai dengan tindakan Hook tertentu dalam siklus hidup target seperti yang didefinisikan dalam spesifikasi Hook.

```
cfn generate
```

Perintah mengembalikan output berikut.

```
Generated files for MyCompany::Testing::MyTestHook
```

Note

Pastikan runtime Lambda Anda up-to-date untuk menghindari penggunaan versi usang. Untuk informasi selengkapnya, lihat [Memperbarui runtime Lambda untuk jenis sumber daya dan Hooks](#).

Langkah 2: Tambahkan Hook handler

Tambahkan kode runtime Hook handler Anda sendiri ke handler yang Anda pilih untuk diterapkan. Misalnya, Anda dapat menambahkan kode berikut untuk logging.

```
LOG.setLevel(logging.INFO)
```

```
LOG.info("Internal testing Hook triggered for target: " +
        request.hookContext.targetName);
```

CloudFormation CLI menghasilkan `src/models.py` file dari file. [Skema konfigurasi](#)

Example `models.py`

```
import sys
from dataclasses import dataclass
from inspect import getmembers, isclass
from typing import (
    AbstractSet,
    Any,
    Generic,
    Mapping,
    MutableMapping,
    Optional,
    Sequence,
    Type,
    TypeVar,
)

from cloudformation_cli_python_lib.interface import (
    BaseModel,
    BaseHookHandlerRequest,
)
from cloudformation_cli_python_lib.recast import recast_object
from cloudformation_cli_python_lib.utils import deserialize_list

T = TypeVar("T")

def set_or_none(value: Optional[Sequence[T]]) -> Optional[AbstractSet[T]]:
    if value:
        return set(value)
    return None

@dataclass
class HookHandlerRequest(BaseHookHandlerRequest):
    pass

@dataclass
```

```

class TypeConfigurationModel(BaseModel):
    limitSize: Optional[str]
    cidr: Optional[str]
    encryptionAlgorithm: Optional[str]

    @classmethod
    def _deserialize(
        cls: Type["_TypeConfigurationModel"],
        json_data: Optional[Mapping[str, Any]],
    ) -> Optional["_TypeConfigurationModel"]:
        if not json_data:
            return None
        return cls(
            limitSize=json_data.get("limitSize"),
            cidr=json_data.get("cidr"),
            encryptionAlgorithm=json_data.get("encryptionAlgorithm"),
        )

_TypeConfigurationModel = TypeConfigurationModel

```

Langkah 3: Menerapkan Hook handler

Dengan kelas data Python yang dihasilkan, Anda dapat menulis penanganan yang benar-benar mengimplementasikan fungsionalitas Hook. Dalam contoh ini, Anda akan menerapkan `preCreate`, `preUpdate`, dan poin `preDelete` pemanggilan untuk penanganan.

Topik

- [Menerapkan handler PreCreate](#)
- [Menerapkan handler preUpdate](#)
- [Menerapkan handler preDelete](#)
- [Menerapkan Hook handler](#)

Menerapkan handler PreCreate

`preCreateHandler` memverifikasi pengaturan enkripsi sisi server untuk sumber daya atau sumber daya. `AWS::S3::Bucket` `AWS::SQS::Queue`

- Untuk `AWS::S3::Bucket` sumber daya, Hook hanya akan lulus jika berikut ini benar.
 - Enkripsi bucket Amazon S3 diatur.

- Kunci bucket Amazon S3 diaktifkan untuk bucket.
- Algoritma enkripsi yang ditetapkan untuk bucket Amazon S3 adalah algoritma yang benar yang diperlukan.
- ID AWS Key Management Service kunci diatur.
- Untuk AWS::SQS::Queue sumber daya, Hook hanya akan lulus jika berikut ini benar.
 - ID AWS Key Management Service kunci diatur.

Menerapkan handler preUpdate

Menerapkan preUpdate handler, yang memulai sebelum operasi update untuk semua target yang ditentukan dalam handler. preUpdateHandler menyelesaikan hal berikut:

- Untuk AWS::S3::Bucket sumber daya, Hook hanya akan lulus jika berikut ini benar:
 - Algoritma enkripsi bucket untuk bucket Amazon S3 belum dimodifikasi.

Menerapkan handler preDelete

Menerapkan preDelete handler, yang memulai sebelum operasi penghapusan untuk semua target yang ditentukan dalam handler. preDeleteHandler menyelesaikan hal berikut:

- Untuk AWS::S3::Bucket sumber daya, Hook hanya akan lulus jika berikut ini benar:
 - Memverifikasi bahwa sumber daya minimum yang sesuai akan ada di akun setelah menghapus sumber daya.
 - Jumlah minimum sumber daya sesuai yang diperlukan diatur dalam konfigurasi Hook.

Menerapkan Hook handler

1. Di IDE Anda, buka `handlers.py` file, yang terletak di `src` folder.
2. Ganti seluruh isi `handlers.py` file dengan kode berikut.

Example handlers.py

```
import logging
from typing import Any, MutableMapping, Optional
import botocore

from cloudformation_cli_python_lib import (
```

```
BaseHookHandlerRequest,
HandlerErrorCode,
Hook,
HookInvocationPoint,
OperationStatus,
ProgressEvent,
SessionProxy,
exceptions,
)

from .models import HookHandlerRequest, TypeConfigurationModel

# Use this logger to forward log messages to CloudWatch Logs.
LOG = logging.getLogger(__name__)
TYPE_NAME = "MyCompany::Testing::MyTestHook"

LOG.setLevel(logging.INFO)

hook = Hook(TYPE_NAME, TypeConfigurationModel)
test_entrypoint = hook.test_entrypoint

def _validate_s3_bucket_encryption(
    bucket: MutableMapping[str, Any], required_encryption_algorithm: str
) -> ProgressEvent:
    status = None
    message = ""
    error_code = None

    if bucket:
        bucket_name = bucket.get("BucketName")

        bucket_encryption = bucket.get("BucketEncryption")
        if bucket_encryption:
            server_side_encryption_rules = bucket_encryption.get(
                "ServerSideEncryptionConfiguration"
            )
            if server_side_encryption_rules:
                for rule in server_side_encryption_rules:
                    bucket_key_enabled = rule.get("BucketKeyEnabled")
                    if bucket_key_enabled:
                        server_side_encryption_by_default = rule.get(
                            "ServerSideEncryptionByDefault"
                        )
```

```

        encryption_algorithm =
server_side_encryption_by_default.get(
            "SSEAlgorithm"
        )
        kms_key_id = server_side_encryption_by_default.get(
            "KMSMasterKeyID"
        ) # "KMSMasterKeyID" is name of the property for an
AWS::S3::Bucket

        if encryption_algorithm == required_encryption_algorithm:
            if encryption_algorithm == "aws:kms" and not
kms_key_id:
                status = OperationStatus.FAILED
                message = f"KMS Key ID not set for bucket with
name: f{bucket_name}"
            else:
                status = OperationStatus.SUCCESS
                message = f"Successfully invoked
PreCreateHookHandler for AWS::S3::Bucket with name: {bucket_name}"
        else:
            status = OperationStatus.FAILED
            message = f"SSE Encryption Algorithm is incorrect for
bucket with name: {bucket_name}"
        else:
            status = OperationStatus.FAILED
            message = f"Bucket key not enabled for bucket with name:
{bucket_name}"

        if status == OperationStatus.FAILED:
            break
    else:
        status = OperationStatus.FAILED
        message = f"No SSE Encryption configurations for bucket with name:
{bucket_name}"
    else:
        status = OperationStatus.FAILED
        message = (
            f"Bucket Encryption not enabled for bucket with name:
{bucket_name}"
        )
    else:
        status = OperationStatus.FAILED
        message = "Resource properties for S3 Bucket target model are empty"

```

```

    if status == OperationStatus.FAILED:
        error_code = HandlerErrorCode.NonCompliant

    return ProgressEvent(status=status, message=message, errorCode=error_code)

def _validate_sqs_queue_encryption(queue: MutableMapping[str, Any]) ->
    ProgressEvent:
    if not queue:
        return ProgressEvent(
            status=OperationStatus.FAILED,
            message="Resource properties for SQS Queue target model are empty",
            errorCode=HandlerErrorCode.NonCompliant,
        )
    queue_name = queue.get("QueueName")

    kms_key_id = queue.get(
        "KmsMasterKeyId"
    ) # "KmsMasterKeyId" is name of the property for an AWS::SQS::Queue
    if not kms_key_id:
        return ProgressEvent(
            status=OperationStatus.FAILED,
            message=f"Server side encryption turned off for queue with name:
{queue_name}",
            errorCode=HandlerErrorCode.NonCompliant,
        )

    return ProgressEvent(
        status=OperationStatus.SUCCESS,
        message=f"Successfully invoked PreCreateHookHandler for
targetAWS::SQS::Queue with name: {queue_name}",
    )

@hook.handler(HookInvocationPoint.CREATE_PRE_PROVISION)
def pre_create_handler(
    session: Optional[SessionProxy],
    request: HookHandlerRequest,
    callback_context: MutableMapping[str, Any],
    type_configuration: TypeConfigurationModel,
) -> ProgressEvent:
    target_name = request.hookContext.targetName
    if "AWS::S3::Bucket" == target_name:

```

```

        return _validate_s3_bucket_encryption(
            request.hookContext.targetModel.get("resourceProperties"),
            type_configuration.encryptionAlgorithm,
        )
    elif "AWS::SQS::Queue" == target_name:
        return _validate_sqs_queue_encryption(
            request.hookContext.targetModel.get("resourceProperties")
        )
    else:
        raise exceptions.InvalidRequest(f"Unknown target type: {target_name}")

def _validate_bucket_encryption_rules_not_updated(
    resource_properties, previous_resource_properties
) -> ProgressEvent:
    bucket_encryption_configs = resource_properties.get("BucketEncryption",
    {}).get(
        "ServerSideEncryptionConfiguration", []
    )
    previous_bucket_encryption_configs = previous_resource_properties.get(
        "BucketEncryption", {}
    ).get("ServerSideEncryptionConfiguration", [])

    if len(bucket_encryption_configs) != len(previous_bucket_encryption_configs):
        return ProgressEvent(
            status=OperationStatus.FAILED,
            message=f"Current number of bucket encryption configs does not
            match previous. Current has {str(len(bucket_encryption_configs))} configs while
            previously there were {str(len(previous_bucket_encryption_configs))} configs",
            errorCode=HandlerErrorCode.NonCompliant,
        )

    for i in range(len(bucket_encryption_configs)):
        current_encryption_algorithm = (
            bucket_encryption_configs[i]
            .get("ServerSideEncryptionByDefault", {})
            .get("SSEAlgorithm")
        )
        previous_encryption_algorithm = (
            previous_bucket_encryption_configs[i]
            .get("ServerSideEncryptionByDefault", {})
            .get("SSEAlgorithm")
        )

```

```

        if current_encryption_algorithm != previous_encryption_algorithm:
            return ProgressEvent(
                status=OperationStatus.FAILED,
                message=f"Bucket Encryption algorithm can not be changed once
set. The encryption algorithm was changed to {current_encryption_algorithm} from
{previous_encryption_algorithm}.",
                errorCode=HandlerErrorCode.NonCompliant,
            )

        return ProgressEvent(
            status=OperationStatus.SUCCESS,
            message="Successfully invoked PreUpdateHookHandler for target:
AWS::SQS::Queue",
        )

def _validate_queue_encryption_not_disabled(
    resource_properties, previous_resource_properties
) -> ProgressEvent:
    if previous_resource_properties.get(
        "KmsMasterKeyId"
    ) and not resource_properties.get("KmsMasterKeyId"):
        return ProgressEvent(
            status=OperationStatus.FAILED,
            errorCode=HandlerErrorCode.NonCompliant,
            message="Queue encryption can not be disable",
        )
    else:
        return ProgressEvent(status=OperationStatus.SUCCESS)

@hook.handler(HookInvocationPoint.UPDATE_PRE_PROVISION)
def pre_update_handler(
    session: Optional[SessionProxy],
    request: BaseHookHandlerRequest,
    callback_context: MutableMapping[str, Any],
    type_configuration: MutableMapping[str, Any],
) -> ProgressEvent:
    target_name = request.hookContext.targetName
    if "AWS::S3::Bucket" == target_name:
        resource_properties =
request.hookContext.targetModel.get("resourceProperties")
        previous_resource_properties = request.hookContext.targetModel.get(
            "previousResourceProperties"

```

```
    )

    return _validate_bucket_encryption_rules_not_updated(
        resource_properties, previous_resource_properties
    )
elif "AWS::SQS::Queue" == target_name:
    resource_properties =
request.hookContext.targetModel.get("resourceProperties")
    previous_resource_properties = request.hookContext.targetModel.get(
        "previousResourceProperties"
    )

    return _validate_queue_encryption_not_disabled(
        resource_properties, previous_resource_properties
    )
else:
    raise exceptions.InvalidRequest(f"Unknown target type: {target_name}")
```

Lanjutkan ke topik berikutnya [Mendaftarkan Hook khusus dengan CloudFormation](#).

Mendaftarkan Hook khusus dengan CloudFormation

Setelah Anda membuat Hook khusus, Anda harus mendaftarkannya CloudFormation sehingga Anda dapat menggunakannya. Di bagian ini, Anda akan belajar mengemas dan mendaftarkan Hook Anda untuk digunakan di bagian Anda Akun AWS.

Package a Hook (Java)

Jika Anda telah mengembangkan Hook Anda dengan Java, gunakan Maven untuk mengemasnya.

Dalam direktori proyek Hook Anda, jalankan perintah berikut untuk membangun Hook Anda, menjalankan pengujian unit, dan paket proyek Anda sebagai JAR file yang dapat Anda gunakan untuk mengirimkan Hook Anda ke CloudFormation registri.

```
mvn clean package
```

Daftarkan Hook kustom

Untuk mendaftarkan Hook

1. (Opsional) Konfigurasi Wilayah AWS nama default Anda ke `us-west-2`, dengan mengirimkan operasi. [configure](#)

```
$ aws configure
AWS Access Key ID [None]: <Your Access Key ID>
AWS Secret Access Key [None]: <Your Secret Key>
Default region name [None]: us-west-2
Default output format [None]: json
```

2. (Opsional) Perintah berikut membangun dan mengemas proyek Hook Anda tanpa mendaftarkannya.

```
$ cfn submit --dry-run
```

3. Daftarkan Hook Anda dengan menggunakan CloudFormation operasi CLI [submit](#).

```
$ cfn submit --set-default
```

Perintah mengembalikan perintah berikut.

```
{'ProgressStatus': 'COMPLETE'}
```

Hasil: Anda telah berhasil mendaftarkan Hook Anda.

Verifikasi Hooks dapat diakses di akun Anda

Verifikasi bahwa Hook Anda tersedia di Akun AWS dan di Wilayah tempat Anda mengirimkannya.

1. Untuk memverifikasi Hook Anda, gunakan [list-types](#) perintah untuk mencantumkan Hook Anda yang baru terdaftar dan kembalikan deskripsi ringkasannya.

```
$ aws cloudformation list-types
```

Perintah mengembalikan output berikut dan juga akan menunjukkan kepada Anda Hooks yang tersedia untuk umum yang dapat Anda aktifkan di Akun AWS dan Wilayah Anda.

```
{
  "TypeSummaries": [
    {
      "Type": "HOOK",
      "TypeName": "MyCompany::Testing::MyTestHook",
      "DefaultVersionId": "00000001",
      "TypeArn": "arn:aws:cloudformation:us-west-2:ACCOUNT_ID/type/hook/MyCompany-Testing-MyTestHook",
      "LastUpdated": "2021-08-04T23:00:03.058000+00:00",
      "Description": "Verifies S3 bucket and SQS queues properties before creating or updating"
    }
  ]
}
```

2. Ambil TypeArn dari list-type output untuk Hook Anda dan simpan.

```
export HOOK_TYPE_ARN=arn:aws:cloudformation:us-west-2:ACCOUNT_ID/type/hook/MyCompany-Testing-MyTestHook
```

Untuk mempelajari cara menerbitkan Hooks untuk penggunaan umum, lihat [Publishing Hooks untuk penggunaan umum](#).

Konfigurasi Kait

Setelah Anda mengembangkan dan mendaftarkan Hook Anda, Anda dapat mengonfigurasi Hook Anda Akun AWS dengan menerbitkannya ke registri.

- Untuk mengkonfigurasi Hook di akun Anda, gunakan [SetTypeConfiguration](#) operasi. Operasi ini memungkinkan properti Hook yang didefinisikan di `properties` bagian skema Hook. Dalam contoh berikut, `minBuckets` properti diatur ke 1 dalam konfigurasi.

Note

Dengan mengaktifkan Hooks di akun Anda, Anda mengotorisasi Hook untuk menggunakan izin yang ditentukan dari Anda. Akun AWS CloudFormation menghapus izin yang tidak diperlukan sebelum meneruskan izin Anda ke Hook. CloudFormation

merekomendasikan pelanggan atau pengguna Hook untuk meninjau izin Hook dan mengetahui izin apa yang diizinkan oleh Hooks sebelum mengaktifkan Hooks di akun Anda.

Tentukan data konfigurasi untuk ekstensi Hook terdaftar Anda di akun yang sama dan Wilayah AWS.

```
$ aws cloudformation set-type-configuration --region us-west-2
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":
{"HookInvocationStatus":"ENABLED","FailureMode":"FAIL","Properties":{"minBuckets":
"1","minQueues": "1", "encryptionAlgorithm": "aws:kms"}}}}'
  --type-arn $HOOK_TYPE_ARN
```

Important

Untuk mengaktifkan Hook Anda untuk secara proaktif memeriksa konfigurasi tumpukan Anda, Anda harus mengatur HookInvocationStatus to ENABLED di HookConfiguration bagian, setelah Hook telah terdaftar dan diaktifkan di akun Anda.

Mengakses AWS APIs di handler

Jika Hooks Anda menggunakan AWS API di salah satu handlernya, CFN-CLI secara otomatis membuat template peran eksekusi IAM, `hook-role.yaml` `hook-role.yaml`Template didasarkan pada izin yang ditentukan untuk setiap handler di bagian handler dari skema Hook. Jika `--role-arn` flag tidak digunakan selama [generate](#) operasi, peran dalam tumpukan ini akan disediakan dan digunakan sebagai peran eksekusi Hook.

Untuk informasi selengkapnya, lihat [Mengakses AWS APIs dari jenis sumber daya](#).

Templat hook-role.yaml

Note

Jika Anda memilih untuk membuat peran eksekusi Anda sendiri, kami sangat menyarankan untuk mempraktikkan prinsip hak istimewa paling sedikit dengan

```
mengizinkan daftar saja hooks.cloudformation.amazonaws.com
danresources.cloudformation.amazonaws.com.
```

Template berikut menggunakan izin IAM, Amazon S3, dan Amazon SQS.

```
AWSTemplateFormatVersion: 2010-09-09
Description: >
  This CloudFormation template creates a role assumed by CloudFormation during
  Hook operations on behalf of the customer.
Resources:
  ExecutionRole:
    Type: 'AWS::IAM::Role'
    Properties:
      MaxSessionDuration: 8400
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - resources.cloudformation.amazonaws.com
                - hooks.cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
        Condition:
          StringEquals:
            aws:SourceAccount: !Ref AWS::AccountId
          StringLike:
            aws:SourceArn: !Sub arn:${AWS::Partition}:cloudformation:
${AWS::Region}:${AWS::AccountId}:type/hook/MyCompany-Testing-MyTestHook/*
      Path: /
    Policies:
      - PolicyName: HookTypePolicy
        PolicyDocument:
          Version: 2012-10-17
          Statement:
            - Effect: Allow
              Action:
                - 's3:GetEncryptionConfiguration'
                - 's3:ListBucket'
                - 's3:ListAllMyBuckets'
                - 'sqs:GetQueueAttributes'
                - 'sqs:GetQueueUrl'
```

```
        - 'sqs:ListQueues'
        Resource: '*'
Outputs:
  ExecutionRoleArn:
    Value: !GetAtt
      - ExecutionRole
      - Arn
```

Menguji Hook kustom di Akun AWS

Sekarang setelah Anda mengkodekan fungsi handler Anda yang sesuai dengan titik pemanggilan, saatnya untuk menguji Hook kustom Anda di tumpukan. CloudFormation

Mode kegagalan Hook disetel ke FAIL jika CloudFormation template tidak menyediakan bucket S3 dengan yang berikut:

- Enkripsi bucket Amazon S3 diatur.
- Kunci bucket Amazon S3 diaktifkan untuk bucket.
- Algoritma enkripsi yang ditetapkan untuk bucket Amazon S3 adalah algoritma yang benar yang diperlukan.
- ID AWS Key Management Service kunci diatur.

Dalam contoh berikut, buat template yang disebut `my-failed-bucket-stack.yml` dengan nama tumpukan `my-hook-stack` yang gagal konfigurasi tumpukan dan berhenti sebelum ketentuan sumber daya.

Menguji Hooks dengan menyediakan tumpukan

Contoh 1: Untuk menyediakan tumpukan

Menyediakan tumpukan yang tidak sesuai

1. Buat template yang menentukan bucket S3. Misalnya, `my-failed-bucket-stack.yml`.

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: AWS::S3::Bucket
    Properties: {}
```

2. Buat tumpukan, dan tentukan template Anda di AWS Command Line Interface (AWS CLI). Dalam contoh berikut, tentukan nama tumpukan sebagai `my-hook-stack` dan nama template sebagai `my-failed-bucket-stack.yml`.

```
$ aws cloudformation create-stack \  
  --stack-name my-hook-stack \  
  --template-body file://my-failed-bucket-stack.yml
```

3. (Opsional) Lihat kemajuan tumpukan Anda dengan menentukan nama tumpukan Anda. Dalam contoh berikut, tentukan nama tumpukan `my-hook-stack`.

```
$ aws cloudformation describe-stack-events \  
  --stack-name my-hook-stack
```

Gunakan `describe-stack-events` operasi untuk melihat kegagalan Hook saat membuat bucket. Berikut ini adalah contoh output dari perintah.

```
{  
  "StackEvents": [  
    ...  
    {  
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-hook-stack/2c693970-f57e-11eb-a0fb-061a2a83f0b9",  
      "EventId": "S3Bucket-CREATE_FAILED-2021-08-04T23:47:03.305Z",  
      "StackName": "my-hook-stack",  
      "LogicalResourceId": "S3Bucket",  
      "PhysicalResourceId": "",  
      "ResourceType": "AWS::S3::Bucket",  
      "Timestamp": "2021-08-04T23:47:03.305000+00:00",  
      "ResourceStatus": "CREATE_FAILED",  
      "ResourceStatusReason": "The following hook(s) failed:  
[MyCompany::Testing::MyTestHook]",  
      "ResourceProperties": "{}",  
      "ClientRequestToken": "Console-CreateStack-abe71ac2-ade4-a762-0499-8d34d91d6a92"  
    },  
    ...  
  ]  
}
```

Hasil: Pemanggilan Hook gagal dalam konfigurasi tumpukan dan menghentikan penyediaan sumber daya.

Gunakan CloudFormation template untuk lulus validasi Hook

1. Untuk membuat tumpukan dan meneruskan validasi Hook, perbarui template sehingga sumber daya Anda menggunakan bucket S3 terenkripsi. Contoh ini menggunakan hal berikut: templat `my-encrypted-bucket-stack.yml`.

```
AWSTemplateFormatVersion: 2010-09-09
Description: |
  This CloudFormation template provisions an encrypted S3 Bucket
Resources:
  EncryptedS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: !Sub encryptedbucket-${AWS::Region}-${AWS::AccountId}
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm: 'aws:kms'
              KMSMasterKeyID: !Ref EncryptionKey
              BucketKeyEnabled: true
  EncryptionKey:
    Type: AWS::KMS::Key
    DeletionPolicy: Retain
    Properties:
      Description: KMS key used to encrypt the resource type artifacts
      EnableKeyRotation: true
      KeyPolicy:
        Version: 2012-10-17
        Statement:
          - Sid: Enable full access for owning account
            Effect: Allow
            Principal:
              AWS: !Ref AWS::AccountId
            Action: 'kms:*'
            Resource: '*'
Outputs:
  EncryptedBucketName:
    Value: !Ref EncryptedS3Bucket
```

Note

Kait tidak akan dipanggil untuk sumber daya yang dilewati.

2. Buat tumpukan dan tentukan template Anda. Dalam contoh ini, nama tumpukan adalah `my-encrypted-bucket-stack`.

```
$ aws cloudformation create-stack \
  --stack-name my-encrypted-bucket-stack \
  --template-body file://my-encrypted-bucket-stack.yml \
```

3. (Opsional) Lihat kemajuan tumpukan Anda dengan menentukan nama tumpukan.

```
$ aws cloudformation describe-stack-events \
  --stack-name my-encrypted-bucket-stack
```

Gunakan `describe-stack-events` perintah untuk melihat respons. Berikut ini adalah contoh perintah `describe-stack-events`.

```
{
  "StackEvents": [
    ...
    {
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
      "EventId": "EncryptedS3Bucket-CREATE_COMPLETE-2021-08-04T23:23:20.973Z",
      "StackName": "my-encrypted-bucket-stack",
      "LogicalResourceId": "EncryptedS3Bucket",
      "PhysicalResourceId": "encryptedbucket-us-west-2-123456789012",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:23:20.973000+00:00",
      "ResourceStatus": "CREATE_COMPLETE",
      "ResourceProperties": "{\"BucketName\":\"encryptedbucket-us-west-2-123456789012\", \"BucketEncryption\":{\"ServerSideEncryptionConfiguration\": [{\"BucketKeyEnabled\":\"true\", \"ServerSideEncryptionByDefault\":{\"SSEAlgorithm\":\"aws:kms\", \"KMSEMasterKeyID\":\"ENCRYPTION_KEY_ARN\"}}]}}",
      "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-b7f6-5661-4e917478d075"
    },
    {
```

```

        "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
        "EventId": "EncryptedS3Bucket-
CREATE_IN_PROGRESS-2021-08-04T23:22:59.410Z",
        "StackName": "my-encrypted-bucket-stack",
        "LogicalResourceId": "EncryptedS3Bucket",
        "PhysicalResourceId": "encryptedbucket-us-west-2-123456789012",
        "ResourceType": "AWS::S3::Bucket",
        "Timestamp": "2021-08-04T23:22:59.410000+00:00",
        "ResourceStatus": "CREATE_IN_PROGRESS",
        "ResourceStatusReason": "Resource creation Initiated",
        "ResourceProperties": "{\"BucketName\": \"encryptedbucket-us-
west-2-123456789012\", \"BucketEncryption\": {\"ServerSideEncryptionConfiguration\":
[ {\"BucketKeyEnabled\": \"true\", \"ServerSideEncryptionByDefault\": {\"SSEAlgorithm
\": \"aws:kms\", \"KMSEncryptionKeyId\": \"ENCRYPTION_KEY_ARN\"} } ] }",
        "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075"
    },
    {
        "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
        "EventId": "EncryptedS3Bucket-6516081f-c1f2-4bfe-a0f0-cefa28679994",
        "StackName": "my-encrypted-bucket-stack",
        "LogicalResourceId": "EncryptedS3Bucket",
        "PhysicalResourceId": "",
        "ResourceType": "AWS::S3::Bucket",
        "Timestamp": "2021-08-04T23:22:58.349000+00:00",
        "ResourceStatus": "CREATE_IN_PROGRESS",
        "ResourceStatusReason": "Hook invocations complete. Resource creation
initiated",
        "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075"
    },
    ...
]
}

```

Hasil: CloudFormation berhasil membuat tumpukan. Logika Hook memverifikasi bahwa AWS::S3::Bucket sumber daya berisi enkripsi sisi server sebelum menyediakan sumber daya.

Contoh 2: Untuk menyediakan tumpukan

Menyediakan tumpukan yang tidak sesuai

1. Buat template yang menentukan bucket S3. Sebagai contoh, `aes256-bucket.yml`.

```
AWSTemplateFormatVersion: 2010-09-09
Description: |
  This CloudFormation template provisions an encrypted S3 Bucket
Resources:
  EncryptedS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: !Sub encryptedbucket-${AWS::Region}-${AWS::AccountId}
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm: AES256
              BucketKeyEnabled: true
Outputs:
  EncryptedBucketName:
    Value: !Ref EncryptedS3Bucket
```

2. Buat tumpukan, dan tentukan template Anda di AWS CLI. Dalam contoh berikut, tentukan nama tumpukan sebagai `my-hook-stack` dan nama template sebagai `aes256-bucket.yml`.

```
$ aws cloudformation create-stack \
  --stack-name my-hook-stack \
  --template-body file://aes256-bucket.yml
```

3. (Opsional) Lihat kemajuan tumpukan Anda dengan menentukan nama tumpukan Anda. Dalam contoh berikut, tentukan nama tumpukan `my-hook-stack`.

```
$ aws cloudformation describe-stack-events \
  --stack-name my-hook-stack
```

Gunakan `describe-stack-events` operasi untuk melihat kegagalan Hook saat membuat bucket. Berikut ini adalah contoh output dari perintah.

```
{
  "StackEvents": [
    ...
```

```

    {
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-hook-stack/2c693970-f57e-11eb-a0fb-061a2a83f0b9",
      "EventId": "S3Bucket-CREATE_FAILED-2021-08-04T23:47:03.305Z",
      "StackName": "my-hook-stack",
      "LogicalResourceId": "S3Bucket",
      "PhysicalResourceId": "",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:47:03.305000+00:00",
      "ResourceStatus": "CREATE_FAILED",
      "ResourceStatusReason": "The following hook(s) failed:
[MyCompany::Testing::MyTestHook]",
      "ResourceProperties": "{}",
      "ClientRequestToken": "Console-CreateStack-abe71ac2-ade4-a762-0499-8d34d91d6a92"
    },
    ...
  ]
}

```

Hasil: Pemanggilan Hook gagal dalam konfigurasi tumpukan dan menghentikan penyediaan sumber daya. Tumpukan gagal karena enkripsi bucket S3 tidak dikonfigurasi dengan benar. Konfigurasi tipe Hook membutuhkan `aws:kms` saat bucket ini digunakan AES256.

Gunakan CloudFormation template untuk lulus validasi Hook

1. Untuk membuat tumpukan dan meneruskan validasi Hook, perbarui template sehingga sumber daya Anda menggunakan bucket S3 terenkripsi. Contoh ini menggunakan hal berikut: templat `kms-bucket-and-queue.yml`.

```

AWSTemplateFormatVersion: 2010-09-09
Description: |
  This CloudFormation template provisions an encrypted S3 Bucket
Resources:
  EncryptedS3Bucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: !Sub encryptedbucket-${AWS::Region}-${AWS::AccountId}
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:

```

```

        SSEAlgorithm: 'aws:kms'
        KMSMasterKeyID: !Ref EncryptionKey
        BucketKeyEnabled: true
    EncryptedQueue:
        Type: AWS::SQS::Queue
        Properties:
            QueueName: !Sub encryptedqueue-${AWS::Region}-${AWS::AccountId}
            KmsMasterKeyId: !Ref EncryptionKey
    EncryptionKey:
        Type: AWS::KMS::Key
        DeletionPolicy: Retain
        Properties:
            Description: KMS key used to encrypt the resource type artifacts
            EnableKeyRotation: true
        KeyPolicy:
            Version: 2012-10-17
            Statement:
                - Sid: Enable full access for owning account
                  Effect: Allow
                  Principal:
                      AWS: !Ref AWS::AccountId
                  Action: 'kms:*'
                  Resource: '*'
    Outputs:
        EncryptedBucketName:
            Value: !Ref EncryptedS3Bucket
        EncryptedQueueName:
            Value: !Ref EncryptedQueue

```

Note

Kait tidak akan dipanggil untuk sumber daya yang dilewati.

2. Buat tumpukan dan tentukan template Anda. Dalam contoh ini, nama tumpukan adalah `my-encrypted-bucket-stack`.

```

$ aws cloudformation create-stack \
  --stack-name my-encrypted-bucket-stack \
  --template-body file://kms-bucket-and-queue.yml

```

3. (Opsional) Lihat kemajuan tumpukan Anda dengan menentukan nama tumpukan.

```
$ aws cloudformation describe-stack-events \
  --stack-name my-encrypted-bucket-stack
```

Gunakan `describe-stack-events` perintah untuk melihat respons. Berikut ini adalah contoh perintah `describe-stack-events`.

```
{
  "StackEvents": [
    ...
    {
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
      "EventId": "EncryptedS3Bucket-
CREATE_COMPLETE-2021-08-04T23:23:20.973Z",
      "StackName": "my-encrypted-bucket-stack",
      "LogicalResourceId": "EncryptedS3Bucket",
      "PhysicalResourceId": "encryptedbucket-us-west-2-123456789012",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:23:20.973000+00:00",
      "ResourceStatus": "CREATE_COMPLETE",
      "ResourceProperties": "{\"BucketName\": \"encryptedbucket-us-
west-2-123456789012\", \"BucketEncryption\": {\"ServerSideEncryptionConfiguration\":
[ {\"BucketKeyEnabled\": \"true\", \"ServerSideEncryptionByDefault\": {\"SSEAlgorithm
\": \"aws:kms\", \"KMSMasterKeyID\": \"ENCRYPTION_KEY_ARN\"} } ] }",
      "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-
b7f6-5661-4e917478d075"
    },
    {
      "StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779",
      "EventId": "EncryptedS3Bucket-
CREATE_IN_PROGRESS-2021-08-04T23:22:59.410Z",
      "StackName": "my-encrypted-bucket-stack",
      "LogicalResourceId": "EncryptedS3Bucket",
      "PhysicalResourceId": "encryptedbucket-us-west-2-123456789012",
      "ResourceType": "AWS::S3::Bucket",
      "Timestamp": "2021-08-04T23:22:59.410000+00:00",
      "ResourceStatus": "CREATE_IN_PROGRESS",
      "ResourceStatusReason": "Resource creation Initiated",
      "ResourceProperties": "{\"BucketName\": \"encryptedbucket-us-
west-2-123456789012\", \"BucketEncryption\": {\"ServerSideEncryptionConfiguration\":
```

```
[{"BucketKeyEnabled": "true", "ServerSideEncryptionByDefault": {"SSEAlgorithm": "aws:kms", "KMSMasterKeyID": "ENCRYPTION_KEY_ARN"}}, {"ClientRequestToken": "Console-CreateStack-39df35ac-ca00-b7f6-5661-4e917478d075"}, {"StackId": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-encrypted-bucket-stack/82a97150-f57a-11eb-8eb2-06a6bdcc7779", "EventId": "EncryptedS3Bucket-6516081f-c1f2-4bfe-a0f0-cefa28679994", "StackName": "my-encrypted-bucket-stack", "LogicalResourceId": "EncryptedS3Bucket", "PhysicalResourceId": "", "ResourceType": "AWS::S3::Bucket", "Timestamp": "2021-08-04T23:22:58.349000+00:00", "ResourceStatus": "CREATE_IN_PROGRESS", "ResourceStatusReason": "Hook invocations complete. Resource creation initiated", "ClientRequestToken": "Console-CreateStack-39df35ac-ca00-b7f6-5661-4e917478d075"}, {"...}]
```

Hasil: CloudFormation berhasil membuat tumpukan. Logika Hook memverifikasi bahwa `AWS::S3::Bucket` sumber daya berisi enkripsi sisi server sebelum menyediakan sumber daya.

Memperbarui Hook kustom

Memperbarui Hook kustom memungkinkan revisi di Hook tersedia di CloudFormation registri.

Untuk memperbarui Hook kustom, kirimkan revisi Anda ke CloudFormation registri melalui operasi CloudFormation [submit](#) CLI.

```
$ cfn submit
```

Untuk menentukan versi default Hook Anda di akun Anda, gunakan [set-type-default-version](#) perintah dan tentukan jenis, jenis nama, dan versi ID.

```
$ aws cloudformation set-type-default-version \
  --type HOOK \
```

```
--type-name MyCompany::Testing::MyTestHook \  
--version-id 00000003
```

Untuk mengambil informasi tentang versi Hook, gunakan [list-type-versions](#).

```
$ aws cloudformation list-type-versions \  
--type HOOK \  
--type-name "MyCompany::Testing::MyTestHook"
```

Membatalkan pendaftaran Hook kustom dari registri CloudFormation

Membatalkan pendaftaran Hook kustom menandai ekstensi atau versi ekstensi seperti DEPRECATED dalam CloudFormation registri, yang menghapusnya dari penggunaan aktif. Setelah usang, Hook kustom tidak dapat digunakan dalam operasi. CloudFormation

Note

Sebelum membatalkan pendaftaran Hook, Anda harus membatalkan pendaftaran secara individual semua versi aktif ekstensi tersebut sebelumnya. Untuk informasi selengkapnya, lihat [DeregisterType](#).

Untuk membatalkan pendaftaran Hook, gunakan [deregister-type](#) operasi dan tentukan ARN Hook Anda.

```
$ aws cloudformation deregister-type \  
--arn HOOK_TYPE_ARN
```

Perintah ini tidak menghasilkan output.

Publishing Hooks untuk penggunaan umum

Untuk mengembangkan Hook pihak ketiga publik, kembangkan Hook Anda sebagai ekstensi pribadi. Kemudian, Wilayah AWS di masing-masing tempat Anda ingin membuat ekstensi tersedia untuk umum:

1. Daftarkan Hook Anda sebagai ekstensi pribadi di CloudFormation registri.
2. Uji Hook Anda untuk memastikannya memenuhi semua persyaratan yang diperlukan untuk dipublikasikan di CloudFormation registri.

3. Publikasikan Hook Anda ke CloudFormation registri.

Note

Sebelum Anda mempublikasikan ekstensi apa pun di Wilayah tertentu, Anda harus terlebih dahulu mendaftarkan sebagai penerbit ekstensi di Wilayah tersebut. Untuk melakukannya di beberapa Wilayah secara bersamaan, lihat [Menerbitkan ekstensi di beberapa Wilayah menggunakan StackSets](#) Panduan Pengguna CloudFormation CLI.

Setelah Anda mengembangkan dan mendaftarkan Hook Anda, Anda dapat membuatnya tersedia untuk umum untuk CloudFormation pengguna umum dengan menerbitkannya ke CloudFormation registri, sebagai ekstensi publik pihak ketiga.

Hooks pihak ketiga publik memungkinkan Anda menawarkan CloudFormation pengguna untuk secara proaktif memeriksa konfigurasi AWS sumber daya sebelum penyediaan. Seperti halnya Hooks pribadi, Hooks publik diperlakukan sama seperti Hook yang diterbitkan oleh AWS dalam CloudFormation

Hooks yang dipublikasikan ke registri terlihat oleh semua CloudFormation pengguna Wilayah AWS di mana mereka diterbitkan. Pengguna kemudian dapat mengaktifkan ekstensi Anda di akun mereka, yang membuatnya tersedia untuk digunakan dalam template mereka. Untuk informasi selengkapnya, lihat [Menggunakan ekstensi publik pihak ketiga dari CloudFormation registri](#) di Panduan CloudFormation Pengguna.

Menguji Hook khusus untuk penggunaan umum

Untuk mempublikasikan Hook kustom terdaftar Anda, itu harus lulus semua persyaratan pengujian yang ditentukan untuk itu. Berikut ini adalah daftar persyaratan yang diperlukan sebelum menerbitkan Hook kustom Anda sebagai ekstensi pihak ketiga.

Setiap handler dan target diuji dua kali. Sekali untuk SUCCESS dan sekali untuk FAILED.

- Untuk kasus SUCCESS respons:
 - Status harus SUCCESS.
 - Tidak boleh mengembalikan kode kesalahan.
 - Penundaan callback harus diatur ke 0 detik, jika ditentukan.
- Untuk kasus FAILED respons:

- Status harus `FAILED`.
- Harus mengembalikan kode kesalahan.
- Harus memiliki pesan sebagai tanggapan.
- Penundaan callback harus diatur ke `0` detik, jika ditentukan.
- Untuk kasus `IN_PROGRESS` respons:
 - Tidak boleh mengembalikan kode kesalahan.
 - `Result` bidang tidak harus diatur sebagai tanggapan.

Menentukan data input untuk digunakan dalam tes kontrak

Secara default, CloudFormation melakukan tes kontrak menggunakan properti input yang dihasilkan dari pola yang Anda tentukan dalam skema Hook Anda. Namun, sebagian besar Hooks cukup kompleks sehingga properti input untuk membuat atau memperbarui tumpukan penyediaan memerlukan pemahaman tentang sumber daya yang disediakan. Untuk mengatasi ini, Anda dapat menentukan input yang CloudFormation digunakan saat melakukan tes kontraknya.

CloudFormation menawarkan dua cara bagi Anda untuk menentukan data input untuk digunakan saat melakukan tes kontrak:

- Mengganti berkas

Menggunakan `overrides` file menyediakan cara ringan untuk menentukan data input untuk properti spesifik tertentu CloudFormation untuk digunakan selama `preCreate`, `preUpdate` dan `preDelete` pengujian operasi.

- Berkas masukan

Anda juga dapat menggunakan beberapa `input` file untuk menentukan data input uji kontrak jika:

- Anda ingin atau perlu menentukan data input yang berbeda untuk membuat, memperbarui, dan menghapus operasi, atau data yang tidak valid untuk menguji.
- Anda ingin menentukan beberapa set data input yang berbeda.

Menentukan data input menggunakan file override

Berikut ini adalah contoh data input Amazon S3 Hook menggunakan `overrides` file.

```
{
```

```
"CREATE_PRE_PROVISION": {
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "/BucketName": "encryptedbucket-us-west-2-contractor",
      "/BucketEncryption/ServerSideEncryptionConfiguration": [
        {
          "BucketKeyEnabled": true,
          "ServerSideEncryptionByDefault": {
            "KMSMasterKeyID": "KMS-KEY-ARN",
            "SSEAlgorithm": "aws:kms"
          }
        }
      ]
    }
  },
  "AWS::SQS::Queue": {
    "resourceProperties": {
      "/QueueName": "MyQueueContract",
      "/KmsMasterKeyId": "hellocontract"
    }
  }
},
"UPDATE_PRE_PROVISION": {
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "/BucketName": "encryptedbucket-us-west-2-contractor",
      "/BucketEncryption/ServerSideEncryptionConfiguration": [
        {
          "BucketKeyEnabled": true,
          "ServerSideEncryptionByDefault": {
            "KMSMasterKeyID": "KMS-KEY-ARN",
            "SSEAlgorithm": "aws:kms"
          }
        }
      ]
    }
  },
  "previousResourceProperties": {
    "/BucketName": "encryptedbucket-us-west-2-contractor",
    "/BucketEncryption/ServerSideEncryptionConfiguration": [
      {
        "BucketKeyEnabled": true,
        "ServerSideEncryptionByDefault": {
          "KMSMasterKeyID": "KMS-KEY-ARN",
          "SSEAlgorithm": "aws:kms"
        }
      ]
    ]
  }
}
```

```

    }
  }
]
},
"INVALID_UPDATE_PRE_PROVISION": {
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "/BucketName": "encryptedbucket-us-west-2-contractor",
      "/BucketEncryption/ServerSideEncryptionConfiguration": [
        {
          "BucketKeyEnabled": true,
          "ServerSideEncryptionByDefault": {
            "KMSMasterKeyId": "KMS-KEY-ARN",
            "SSEAlgorithm": "AES256"
          }
        }
      ]
    },
    "previousResourceProperties": {
      "/BucketName": "encryptedbucket-us-west-2-contractor",
      "/BucketEncryption/ServerSideEncryptionConfiguration": [
        {
          "BucketKeyEnabled": true,
          "ServerSideEncryptionByDefault": {
            "KMSMasterKeyId": "KMS-KEY-ARN",
            "SSEAlgorithm": "aws:kms"
          }
        }
      ]
    }
  }
},
"INVALID": {
  "AWS::SQS::Queue": {
    "resourceProperties": {
      "/QueueName": "MyQueueContract",
      "/KmsMasterKeyId": "KMS-KEY-ARN"
    }
  }
}
}

```

Menentukan data input menggunakan file input

Gunakan `input` file untuk menentukan berbagai jenis data input CloudFormation untuk digunakan: `preCreate` input, `preUpdate` input, dan input tidak valid. Setiap jenis data ditentukan dalam file terpisah. Anda juga dapat menentukan beberapa set data input untuk tes kontrak.

Untuk menentukan `input` file yang akan CloudFormation digunakan dalam pengujian kontrak, tambahkan `inputs` folder ke direktori root proyek Hooks Anda. Kemudian tambahkan file input Anda.

Tentukan jenis data input yang berisi file dengan menggunakan konvensi penamaan berikut, di mana bilangan bulat:

- `inputs_n_pre_create.json`: Gunakan file dengan `preCreate` penanganan untuk menentukan input untuk membuat sumber daya.
- `inputs_n_pre_update.json`: Gunakan file dengan `preUpdate` penanganan untuk menentukan input untuk memperbarui sumber daya.
- `inputs_n_pre_delete.json`: Gunakan file dengan `preDelete` penanganan untuk menentukan input untuk menghapus sumber daya.
- `inputs_n_invalid.json`: Untuk menentukan input yang tidak valid untuk diuji.

Untuk menentukan beberapa set data masukan untuk pengujian kontrak, tambahkan bilangan bulat dalam nama file untuk mengurutkan kumpulan data masukan Anda. Misalnya, kumpulan file input pertama Anda harus diberi nama `inputs_1_pre_create.json`, `inputs_1_pre_update.json`, dan `inputs_1_pre_invalid.json`. Set Anda berikutnya akan diberi nama `inputs_2_pre_create.json`, `inputs_2_pre_update.json`, dan `inputs_2_pre_invalid.json`, dan seterusnya.

Setiap file input adalah file JSON yang hanya berisi properti sumber daya yang akan digunakan dalam pengujian.

Berikut ini adalah direktori contoh `inputs` untuk Amazon S3 menentukan data input menggunakan file input.

`inputs_1_pre_create.json`

Berikut ini adalah contoh dari tes `inputs_1_pre_create.json` kontrak.

```
{
```

```

    "AWS::S3::Bucket": {
      "resourceProperties": {
        "AccessControl": "BucketOwnerFullControl",
        "AnalyticsConfigurations": [],
        "BucketEncryption": {
          "ServerSideEncryptionConfiguration": [
            {
              "BucketKeyEnabled": true,
              "ServerSideEncryptionByDefault": {
                "KMSMasterKeyId": "KMS-KEY-ARN",
                "SSEAlgorithm": "aws:kms"
              }
            }
          ]
        },
        "BucketName": "encryptedbucket-us-west-2"
      }
    },
    "AWS::SQS::Queue": {
      "resourceProperties": {
        "QueueName": "MyQueue",
        "KmsMasterKeyId": "KMS-KEY-ARN"
      }
    }
  }
}

```

inputs_1_pre_update.json

Berikut ini adalah contoh dari tes inputs_1_pre_update.json kontrak.

```

{
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
            "BucketKeyEnabled": true,
            "ServerSideEncryptionByDefault": {
              "KMSMasterKeyId": "KMS-KEY-ARN",
              "SSEAlgorithm": "aws:kms"
            }
          }
        ]
      },

```

```

    "BucketName": "encryptedbucket-us-west-2"
  },
  "previousResourceProperties": {
    "BucketEncryption": {
      "ServerSideEncryptionConfiguration": [
        {
          "BucketKeyEnabled": true,
          "ServerSideEncryptionByDefault": {
            "KMSEncryption": {
              "KMSMasterKeyID": "KMS-KEY-ARN",
              "SSEAlgorithm": "aws:kms"
            }
          }
        }
      ]
    },
    "BucketName": "encryptedbucket-us-west-2"
  }
}

```

inputs_1_invalid.json

Berikut ini adalah contoh dari tes `inputs_1_invalid.json` kontrak.

```

{
  "AWS::S3::Bucket": {
    "resourceProperties": {
      "AccessControl": "BucketOwnerFullControl",
      "AnalyticsConfigurations": [],
      "BucketEncryption": {
        "ServerSideEncryptionConfiguration": [
          {
            "ServerSideEncryptionByDefault": {
              "SSEAlgorithm": "AES256"
            }
          }
        ]
      },
      "BucketName": "encryptedbucket-us-west-2"
    }
  },
  "AWS::SQS::Queue": {
    "resourceProperties": {
      "NotValid": "The property of this resource is not valid."
    }
  }
}

```

```
}  
}
```

inputs_1_invalid_pre_update.json

Berikut ini adalah contoh dari tes `inputs_1_invalid_pre_update.json` kontrak.

```
{  
  "AWS::S3::Bucket": {  
    "resourceProperties": {  
      "BucketEncryption": {  
        "ServerSideEncryptionConfiguration": [  
          {  
            "BucketKeyEnabled": true,  
            "ServerSideEncryptionByDefault": {  
              "KMSMasterKeyID": "KMS-KEY-ARN",  
              "SSEAlgorithm": "AES256"  
            }  
          }  
        ]  
      },  
      "BucketName": "encryptedbucket-us-west-2"  
    },  
    "previousResourceProperties": {  
      "BucketEncryption": {  
        "ServerSideEncryptionConfiguration": [  
          {  
            "BucketKeyEnabled": true,  
            "ServerSideEncryptionByDefault": {  
              "KMSMasterKeyID": "KMS-KEY-ARN",  
              "SSEAlgorithm": "aws:kms"  
            }  
          }  
        ]  
      },  
      "BucketName": "encryptedbucket-us-west-2"  
    }  
  }  
}
```

Untuk informasi selengkapnya, lihat [Menerbitkan ekstensi agar tersedia untuk penggunaan umum](#) di Panduan Pengguna CloudFormation CLI.

Referensi sintaks skema untuk Hooks CloudFormation

Bagian ini menjelaskan sintaks skema yang Anda gunakan untuk mengembangkan CloudFormation Hooks.

Hook mencakup spesifikasi Hook yang diwakili oleh skema JSON dan penanganan Hook. Langkah pertama dalam membuat Hook kustom adalah pemodelan skema yang mendefinisikan Hook, propertinya, dan atributnya. Saat Anda menginisialisasi proyek Hook kustom menggunakan perintah CloudFormation [initCLI](#), file skema Hook dibuat untuk Anda. Gunakan file skema ini sebagai titik awal untuk menentukan bentuk dan semantik Hook kustom Anda.

Skema sintaks

Skema berikut adalah struktur untuk Hook.

```
{
  "typeName": "string",
  "description": "string",
  "sourceUrl": "string",
  "documentationUrl": "string",
  "definitions": {
    "definitionName": {
      . . .
    }
  },
  "typeConfiguration": {
    "properties": {
      "propertyName": {
        "description": "string",
        "type": "string",
        . . .
      },
    },
  },
  "required": [
    "propertyName"
    . . .
  ],
  "additionalProperties": false
},
"handlers": {
  "preCreate": {
    "targetNames": [
```

```
    ],
    "permissions": [
    ]
  },
  "preUpdate": {
    "targetNames": [
    ],
    "permissions": [
    ]
  },
  "preDelete": {
    "targetNames": [
    ],
    "permissions": [
    ]
  }
},
"additionalProperties": false
}
```

typeName

Nama unik untuk Hook Anda. Menentukan namespace tiga bagian untuk Hook Anda, dengan pola yang direkomendasikan. `Organization::Service::Hook`

Note

Ruang nama organisasi berikut dicadangkan dan tidak dapat digunakan dalam nama tipe Hook Anda:

- Alexa
- AMZN
- Amazon
- ASK
- AWS
- Custom
- Dev

Wajib: Ya

Pola: `^[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}$`

Minimal: 10

Maksimum: 196

description

Deskripsi singkat tentang Hook yang ditampilkan di CloudFormation konsol.

Wajib: Ya

sourceUrl

URL kode sumber untuk Hook, jika publik.

Wajib: Tidak

Maksimum: 4096

documentationUrl

URL halaman yang menyediakan dokumentasi rinci untuk Hook.

Wajib: Ya

Pola: `^https\:\/\/[0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])(\:[0-9]*)*([\?/#].*)?$`

Maksimum: 4096

Note

Meskipun skema Hook harus menyertakan deskripsi properti yang lengkap dan akurat, Anda dapat menggunakan `documentationURL` properti untuk memberikan detail lebih lanjut kepada pengguna, termasuk contoh, kasus penggunaan, dan informasi terperinci lainnya.

definitions

Gunakan `definitions` blok untuk menyediakan skema properti Hook bersama.

Ini dianggap sebagai praktik terbaik untuk menggunakan `definitions` bagian untuk menentukan elemen skema yang dapat digunakan di beberapa titik dalam skema tipe Hook Anda.

Anda kemudian dapat menggunakan pointer JSON untuk mereferensikan elemen itu di tempat yang sesuai dalam skema tipe Hook Anda.

Wajib: Tidak

`typeConfiguration`

Definisi data konfigurasi Hook.

Wajib: Ya

`properties`

Sifat-sifat Hook. Semua properti Hook harus dinyatakan dalam skema. Sejajarkan properti skema Hook dengan properti konfigurasi tipe Hook.

Note

Properti bersarang tidak diizinkan. Sebagai gantinya, tentukan properti bersarang dalam `definitions` elemen, dan gunakan `$ref` penunjuk untuk mereferensikannya di properti yang diinginkan.

Properti berikut saat ini didukung:

- `default`— Nilai default properti.
- `description`— Deskripsi properti.
- `pattern`— Pola regex yang digunakan untuk memvalidasi input.
- `type`— Jenis properti yang diterima.

`additionalProperties`

`additionalProperties` harus diatur ke `false`. Semua properti Hook harus dinyatakan dalam skema: input arbitrer tidak diperbolehkan.


Wajib: Ya

Nilai yang valid: `false`

`handlers`

Handler menentukan operasi yang dapat memulai Hook didefinisikan dalam skema, seperti titik pemanggilan Hook. Misalnya, `preUpdate` handler dipanggil sebelum operasi pembaruan untuk semua target yang ditentukan di handler.

Nilai yang valid: `preCreate` | `preUpdate` | `preDelete`

 Note

Setidaknya satu nilai harus ditentukan untuk handler.

 Important

Operasi tumpukan yang menghasilkan status `UpdateCleanup` jangan memanggil Hook. Misalnya, selama dua skenario berikut, `preDelete` handler Hook tidak dipanggil:

- tumpukan diperbarui setelah menghapus satu sumber daya dari template.
- sumber daya dengan jenis [penggantian](#) pembaruan dihapus.

targetNames

Sebuah array string nama tipe yang Hook target. Misalnya, jika `preCreate` handler memiliki `AWS::S3::Bucket` target, Hook berjalan untuk bucket Amazon S3 selama fase provisioning.


- `TargetName`

Tentukan setidaknya satu nama target untuk setiap handler yang diterapkan.

Pola: `^[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}$`

Minimal: 1

Wajib: Ya

 Warning

Referensi dinamis SSM `SecureString` dan `Secrets Manager` tidak diselesaikan sebelum diteruskan ke Hooks.

permissions

Sebuah array string yang menentukan AWS izin yang diperlukan untuk memanggil handler.

Wajib: Ya

additionalProperties

`additionalProperties` harus diatur ke `false`. Semua properti Hook harus dinyatakan dalam skema: input arbitrer tidak diperbolehkan.

Wajib: Ya

Nilai yang valid: `false`

Contoh skema Hooks

Contoh 1

Penelusuran Java dan Python menggunakan contoh kode berikut. Berikut ini adalah contoh struktur untuk Hook yang disebut `mycompany-testing-mytesthook.json`.

```
{
  "typeName": "MyCompany::Testing::MyTestHook",
  "description": "Verifies S3 bucket and SQS queues properties before create and
update",
  "sourceUrl": "https://mycorp.com/my-repo.git",
  "documentationUrl": "https://mycorp.com/documentation",
  "typeConfiguration": {
    "properties": {
      "minBuckets": {
        "description": "Minimum number of compliant buckets",
        "type": "string"
      },
      "minQueues": {
        "description": "Minimum number of compliant queues",
        "type": "string"
      },
      "encryptionAlgorithm": {
        "description": "Encryption algorithm for SSE",
        "default": "AES256",
        "type": "string",
        "pattern": "[a-zA-Z]*[1-9]"
      }
    },
    "required": [
  ],
```

```
    "additionalProperties":false
  },
  "handlers":{
    "preCreate":{
      "targetNames":[
        "AWS::S3::Bucket",
        "AWS::SQS::Queue"
      ],
      "permissions":[
        ]
    },
    "preUpdate":{
      "targetNames":[
        "AWS::S3::Bucket",
        "AWS::SQS::Queue"
      ],
      "permissions":[
        ]
    },
    "preDelete":{
      "targetNames":[
        "AWS::S3::Bucket",
        "AWS::SQS::Queue"
      ],
      "permissions":[
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetEncryptionConfiguration",
        "sqs:ListQueues",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ]
    }
  },
  "additionalProperties":false
}
```

Contoh 2

Contoh berikut adalah skema yang menggunakan STACK dan CHANGE_SET targetNames untuk menargetkan template tumpukan dan operasi set perubahan.

```
{
  "typeName": "MyCompany::Testing::MyTestHook",
  "description": "Verifies Stack and Change Set properties before create and update",
  "sourceUrl": "https://mycorp.com/my-repo.git",
  "documentationUrl": "https://mycorp.com/documentation",
  "typeConfiguration": {
    "properties": {
      "minBuckets": {
        "description": "Minimum number of compliant buckets",
        "type": "string"
      },
      "minQueues": {
        "description": "Minimum number of compliant queues",
        "type": "string"
      },
      "encryptionAlgorithm": {
        "description": "Encryption algorithm for SSE",
        "default": "AES256",
        "type": "string",
        "pattern": "[a-zA-Z]*[1-9]"
      }
    },
    "required": [
    ],
    "additionalProperties": false
  },
  "handlers": {
    "preCreate": {
      "targetNames": [
        "STACK",
        "CHANGE_SET"
      ],
      "permissions": [
      ]
    },
    "preUpdate": {
      "targetNames": [
        "STACK"
      ],
      "permissions": [
      ]
    },
    "preDelete": {
```

```
        "targetNames":[
            "STACK"
        ],
        "permissions":[
            ]
    }
},
"additionalProperties":false
}
```

Nonaktifkan dan aktifkan CloudFormation Hooks

Topik ini menjelaskan cara menonaktifkan dan kemudian mengaktifkan kembali Hook untuk sementara mencegahnya aktif di akun Anda. Menonaktifkan Hooks dapat berguna ketika Anda perlu menyelidiki masalah tanpa gangguan dari Hooks.

Nonaktifkan dan aktifkan Hook di akun Anda (konsol)

Untuk menonaktifkan Hook di akun Anda

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Hook berada.
3. Dari panel navigasi, pilih Hooks.
4. Pilih nama Hook yang ingin Anda nonaktifkan.
5. Pada halaman detail Hook, di sebelah kanan nama Hook, pilih tombol Nonaktifkan.
6. Saat diminta konfirmasi, pilih Nonaktifkan Hook.

Untuk mengaktifkan kembali Hook yang dinonaktifkan sebelumnya

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Hook berada.
3. Dari panel navigasi, pilih Hooks.
4. Pilih nama Hook yang ingin Anda aktifkan.
5. Pada halaman Hook details, di sebelah kanan nama Hook, pilih tombol Enable.
6. Saat diminta konfirmasi, pilih Aktifkan Hook.

Nonaktifkan dan aktifkan Hook di akun Anda (AWS CLI)

Important

AWS CLI Perintah untuk menonaktifkan dan mengaktifkan Hooks menggantikan seluruh konfigurasi Hook dengan nilai yang ditentukan dalam opsi. `--configuration` Untuk

menghindari perubahan yang tidak diinginkan, Anda harus menyertakan semua pengaturan yang ada yang ingin Anda pertahankan saat menjalankan perintah ini. Untuk melihat data konfigurasi saat ini, gunakan [describe-type](#) perintah.

Untuk menonaktifkan Hook

Gunakan [set-type-configuration](#) perintah berikut dan tentukan HookInvocationStatus DISABLED untuk menonaktifkan Hook. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation set-type-configuration \
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":
{"HookInvocationStatus": "DISABLED", "FailureMode": "FAIL",
"TargetOperations": ["STACK", "RESOURCE", "CHANGE_SET"], "Properties":{}}}}' \
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \
  --region us-west-2
```

Untuk mengaktifkan kembali Hook yang dinonaktifkan sebelumnya

Gunakan [set-type-configuration](#) perintah berikut dan tentukan HookInvocationStatus ENABLED untuk mengaktifkan kembali Hook. Ganti placeholder dengan nilai spesifik Anda.

```
aws cloudformation set-type-configuration \
  --configuration '{"CloudFormationConfiguration":{"HookConfiguration":
{"HookInvocationStatus": "ENABLED", "FailureMode": "FAIL",
"TargetOperations": ["STACK", "RESOURCE", "CHANGE_SET"], "Properties":{}}}}' \
  --type-arn "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyTestHook" \
  --region us-west-2
```

Lihat informasi yang lebih lengkap di [Referensi sintaks skema konfigurasi hook](#).

Lihat hasil pemanggilan untuk Hooks CloudFormation

Topik ini menjelaskan cara melihat hasil pemanggilan untuk CloudFormation Hooks. Melihat hasil pemanggilan dapat membantu Anda memahami cara Hooks mengevaluasi sumber daya Anda dan menyelesaikan masalah apa pun yang terdeteksi saat Hooks memverifikasi sumber daya.

Pemanggilan adalah contoh spesifik ketika logika validasi Anda (apakah itu kontrol AWS Control Tower proaktif, aturan Penjaga, atau fungsi Lambda) berjalan selama siklus hidup sumber daya.

Lihat hasil pemanggilan di konsol

Anda dapat melihat hasil pemanggilan di konsol dengan tiga cara: melalui halaman ringkasan Pemanggilan, melalui riwayat pemanggilan untuk masing-masing Hook, atau melalui peristiwa tumpukan individual untuk pemanggilan khusus tumpukan.

Lihat hasil untuk semua Hooks

Halaman ringkasan Doa memberikan tampilan komprehensif dari semua pemanggilan Hook di seluruh akun dan Wilayah Anda selama 90 hari terakhir.

Untuk melihat hasil untuk semua Hooks

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Anda ingin melihat pemanggilan Hook.
3. Dari panel navigasi, pilih Ringkasan pemanggilan.
4. Halaman ini menampilkan daftar semua pemanggilan Hook dari 90 hari terakhir, termasuk:
 - ID invokasi
 - Kait
 - Target
 - Mode (WarnatauFail)
 - Hasil (Warning,Pass,Failed,In progress)
 - Waktu invokasi

- Pesan hasil
5. Anda dapat memfilter daftar menggunakan bilah pencarian di bagian atas tabel untuk menemukan pemanggilan tertentu.
 6. Pilih pemanggilan tertentu untuk melihat detail tambahan lainnya tentang hasil pemanggilan, termasuk panduan remediasi untuk pemanggilan Hook yang gagal.

Lihat riwayat pemanggilan untuk masing-masing Hooks

Anda juga dapat melihat hasil pemanggilan melalui riwayat pemanggilan untuk masing-masing Hooks.

Untuk melihat pemanggilan Hook untuk Hook tertentu

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat Anda ingin melihat pemanggilan Hook.
3. Dari panel navigasi, pilih Hooks.
4. Pilih Hook yang ingin Anda lihat pemanggilan Hook.
5. Pilih pemanggilan tertentu untuk melihat detail tambahan lainnya tentang hasil pemanggilan, termasuk panduan remediasi untuk pemanggilan Hook yang gagal.

Lihat hasil untuk pemanggilan khusus tumpukan

Anda juga dapat melihat hasil pemanggilan untuk tumpukan tertentu melalui halaman Stack Events.

Untuk melihat pemanggilan Hook untuk tumpukan tertentu

1. Masuk ke Konsol Manajemen AWS dan buka CloudFormation konsol di <https://console.aws.amazon.com/cloudformation>.
2. Pada bilah navigasi di bagian atas layar, pilih Wilayah AWS tempat operasi tumpukan terjadi.
3. Dari panel navigasi, pilih Stacks.
4. Pilih tumpukan yang ingin Anda lihat pemanggilan Hook.
5. Pilih tab Stack events.
6. Dalam daftar peristiwa, cari acara dengan pemanggilan Hook lengkap di kolom Alasan status.

7. Untuk melihat detail pemanggilan Hook tertentu, tinjau kolom pemanggilan Hook, dan pilih teks yang digarisbawahi untuk membuka jendela pop-up dengan informasi lebih rinci.

Note

Untuk menampilkan kolom tersembunyi, pilih ikon roda gigi di sudut kanan atas bagian untuk membuka modal Preferensi, perbarui pengaturan sesuai kebutuhan, dan pilih Konfirmasi.

Lihat hasil pemanggilan menggunakan AWS CLI

Gunakan [list-hook-results](#) perintah untuk mengambil informasi tentang pemanggilan Hook. Perintah ini mendukung opsi penyaringan berikut:

- Dapatkan semua hasil pemanggilan Hook (tidak diperlukan parameter)
- Filter oleh Hook ARN (gunakan `--type-arn`)
- Filter berdasarkan Hook ARN dan status (gunakan `--type-arn` dan `--status`)
- Cari target tertentu (penggunaan `--target-type` dan `--target-id`)

Filter hasil oleh Hook ARN

Perintah berikut mencantumkan semua hasil pemanggilan Hook untuk Hook tertentu.

```
aws cloudformation list-hook-results \  
  --type-arn arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-Security-ComplianceHook \  
  --region us-west-2
```

Contoh output:

```
{  
  "HookResults": [  
    {  
      "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-Security-ComplianceHook",  
      "HookResultId": "59ef501c-0ac4-47c0-a193-e071cabf748d",  
      "TypeName": "MyOrg::Security::ComplianceHook",  
      "TypeVersionId": "00000001",
```

```

    "HookExecutionTarget": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/39f29d10-73ed-11f0-abc1-0affdfe4aebb",
    "InvokedAt": "2025-08-08T00:18:39.651Z",
    "FailureMode": "WARN",
    "HookStatusReason": "...",
    "InvocationPoint": "PRE_PROVISION",
    "Status": "HOOK_COMPLETE_FAILED"
  },
  ...
]
}

```

Untuk deskripsi bidang dalam respons, lihat [HookResultSummary](#) di Referensi AWS CloudFormation API.

Filter hasil berdasarkan Hook ARN dan status

Untuk memfilter status umum di antara hasil, tentukan `--status` opsi dalam perintah. Nilai yang valid adalah:

- `HOOK_IN_PROGRESS`: Hook sedang berjalan.
- `HOOK_COMPLETE_SUCCEEDED`: The Hook berhasil diselesaikan.
- `HOOK_COMPLETE_FAILED`: Hook selesai tetapi validasi gagal.
- `HOOK_FAILED`: Hook mengalami kesalahan selama eksekusi.

```

aws cloudformation list-hook-results \
  --type-arn arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-Security-
ComplianceHook \
  --status HOOK_COMPLETE_FAILED \
  --region us-west-2

```

Contoh output:

```

{
  "HookResults": [
    {
      "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-
Security-ComplianceHook",
      "HookResultId": "59ef501c-0ac4-47c0-a193-e071cabf748d",
      "TypeName": "MyOrg::Security::ComplianceHook",

```

```

    "TypeVersionId": "00000001",
    "HookExecutionTarget": "arn:aws:cloudformation:us-west-2:123456789012:stack/my-
stack/39f29d10-73ed-11f0-abc1-0affdfe4aebb",
    "InvokedAt": "2025-08-08T00:18:39.651Z",
    "FailureMode": "WARN",
    "HookStatusReason": "...",
    "InvocationPoint": "PRE_PROVISION",
    "Status": "HOOK_COMPLETE_FAILED"
  },
  ...
]
}

```

Untuk deskripsi bidang dalam respons, lihat [HookResultSummary](#) di Referensi AWS CloudFormation API.

Filter hasil berdasarkan jenis target dan ID target

Perintah berikut mencantumkan semua hasil pemanggilan Hook untuk permintaan Cloud Control API tertentu.

```

aws cloudformation list-hook-results \
  --target-type CLOUD_CONTROL \
  --target-id d417b05b-9eff-46ef-b164-08c76aec1801 \
  --region us-west-2

```

Contoh output:

```

{
  "HookResults": [
    {
      "TargetType": "CLOUD_CONTROL",
      "TargetId": "d417b05b-9eff-46ef-b164-08c76aec1801",
      "HookResults": [
        {
          "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-
Security-ComplianceHook",
          "HookResultId": "4e7f4766-d8fe-44e5-8587-5b327a148abe",
          "TypeName": "MyOrg::Security::ComplianceHook",
          "TypeVersionId": "00000001",
          "FailureMode": "WARN",
          "HookStatusReason": "...",

```

```

        "InvocationPoint": "PRE_PROVISION",
        "Status": "HOOK_COMPLETE_FAILED"
    },
    ...
]
}
]
}

```

Untuk deskripsi bidang dalam respons, lihat [HookResultSummary](#) di Referensi AWS CloudFormation API.

Dapatkan hasil terperinci untuk pemanggilan tertentu

Gunakan [get-hook-result](#) perintah untuk mengambil informasi rinci tentang pemanggilan Hook tertentu, termasuk anotasi dengan hasil pemeriksaan kepatuhan dan panduan remediasi.

```

aws cloudformation get-hook-result \
  --hook-result-id 59ef501c-0ac4-47c0-a193-e071cabf748d \
  --region us-west-2

```

Contoh output:

```

{
  "HookResultId": "59ef501c-0ac4-47c0-a193-e071cabf748d",
  "InvocationPoint": "PRE_PROVISION",
  "FailureMode": "WARN",
  "TypeName": "MyOrg::Security::ComplianceHook",
  "TypeVersionId": "00000001",
  "TypeArn": "arn:aws:cloudformation:us-west-2:123456789012:type/hook/MyOrg-Security-ComplianceHook",
  "Status": "HOOK_COMPLETE_FAILED",
  "HookStatusReason": "Hook completed with failed validations",
  "InvokedAt": "2025-08-08T00:18:39.651Z",
  "Target": {
    "TargetType": "RESOURCE",
    "TargetTypeName": "AWS::S3::Bucket",
    "TargetId": "my-s3-bucket",
    "Action": "CREATE"
  },
  "Annotations": [
    {

```

```
"AnnotationName": "BlockPublicAccessCheck",
"Status": "FAILED",
"StatusMessage": "Bucket does not block public access",
"RemediationMessage": "Enable block public access settings on the S3 bucket",
"SeverityLevel": "HIGH"
},
{
"AnnotationName": "BucketEncryptionCheck",
"Status": "PASSED",
"StatusMessage": "Bucket has encryption configured correctly"
}
]
}
```

Untuk deskripsi bidang dalam respons, lihat [GetHookResult](#) di Referensi AWS CloudFormation API.

Referensi sintaks skema konfigurasi hook

Bagian ini menguraikan sintaks skema yang digunakan untuk mengkonfigurasi Hooks.

CloudFormation menggunakan skema konfigurasi ini saat runtime saat menjalankan Hook di file. Akun AWS

Untuk mengaktifkan Hook Anda secara proaktif memeriksa konfigurasi tumpukan Anda, atur `HookInvocationStatus` ke `ENABLED` setelah Hook terdaftar dan diaktifkan di akun Anda.

Topik

- [Properti skema konfigurasi kait](#)
- [Contoh konfigurasi kait](#)
- [CloudFormation Filter tingkat tumpukan kait](#)
- [CloudFormation Filter target kait](#)
- [Menggunakan wildcard dengan nama target Hook](#)

Note

Jumlah maksimum data yang dapat disimpan oleh konfigurasi Hook adalah 300 KB. Ini adalah tambahan untuk semua kendala yang dikenakan pada parameter `Configuration` permintaan operasi. [SetTypeConfiguration](#)

Properti skema konfigurasi kait

Skema berikut adalah struktur untuk skema konfigurasi Hook.

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": ["STACK"],
      "FailureMode": "FAIL",
      "EncryptionConfiguration": {
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/abc-123"
      }
    }
  },
}
```

```

    "Properties": {
      ...
    }
  }
}

```

HookConfiguration

Konfigurasi Hook mendukung pengaktifan atau penonaktifan Hooks pada tingkat tumpukan, mode kegagalan, dan nilai properti Hook.

Konfigurasi Hook mendukung properti berikut.

HookInvocationStatus

Menentukan apakah Hook adalah ENABLED atau DISABLED.

Nilai yang valid: ENABLED | DISABLED

TargetOperations

Menentukan daftar operasi Hook dijalankan terhadap. Untuk informasi selengkapnya, lihat [Target kait](#).

Nilai yang valid: STACK | RESOURCE | CHANGE_SET | CLOUD_CONTROL

TargetStacks

Tersedia untuk kompatibilitas mundur. Gunakan *HookInvocationStatus* sebagai gantinya.

Jika mode diatur ke ALL, Hook berlaku untuk semua tumpukan di akun Anda selama operasi CREATE, UPDATE, atau DELETE sumber daya.

Jika mode diatur ke NONE, Hook tidak akan berlaku untuk tumpukan di akun Anda.

Nilai yang valid: ALL | NONE

FailureMode

Bidang ini memberi tahu layanan bagaimana memperlakukan kegagalan Hook.

- Jika mode diatur ke FAIL, dan Hook gagal, maka konfigurasi gagal berhenti menyediakan sumber daya dan memutar kembali tumpukan.

- Jika mode diatur ke WARN dan Hook gagal, maka konfigurasi peringatan memungkinkan penyediaan untuk melanjutkan dengan pesan peringatan.

Nilai yang valid: FAIL | WARN

EncryptionConfiguration

Menentukan pengaturan enkripsi untuk data anotasi Hook.

KmsKeyId

Alias, alias ARN, ID kunci, atau ARN kunci dari kunci enkripsi simetris yang digunakan untuk mengenkripsi data AWS KMS anotasi Hook. Untuk informasi lebih lanjut, lihat [KeyId](#) di AWS KMS dokumen.

Sebelum Anda dapat membuat Hooks dengan AWS KMS kunci yang dikelola pelanggan, pengguna atau peran Anda harus memiliki AWS KMS izin untuk DescribeKey dan GenerateDataKey Untuk informasi selengkapnya, lihat [AWS KMS kebijakan kunci dan izin untuk mengenkripsi hasil CloudFormation Hooks saat istirahat](#).

Properties

Menentukan properti runtime Hook. Ini harus sesuai dengan bentuk properti yang didukung oleh skema Hooks.

Contoh konfigurasi kait

Untuk contoh konfigurasi Hooks dari AWS CLI, lihat bagian berikut:

- [Aktifkan Hook \(\) berbasis kontrol proaktif AWS CLI](#)
- [Aktifkan Guard Hook \(AWS CLI\)](#)
- [Aktifkan Lambda Hook \(\)AWS CLI](#)

CloudFormation Filter tingkat tumpukan kait

Anda dapat menambahkan filter tingkat tumpukan ke CloudFormation Hooks Anda untuk menargetkan tumpukan tertentu berdasarkan nama dan peran tumpukan. Ini berguna dalam kasus di mana Anda memiliki beberapa tumpukan dengan jenis sumber daya yang sama, tetapi Hook ditujukan untuk tumpukan tertentu.

Bagian ini menjelaskan cara kerja filter ini dan memberikan contoh yang dapat Anda ikuti.

Struktur dasar konfigurasi Hook tanpa penyaringan tingkat tumpukan terlihat seperti ini:

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "TargetFilters": {
        "Actions": [
          "CREATE",
          "UPDATE",
          "DELETE"
        ]
      }
    }
  }
}
```

Untuk informasi selengkapnya tentang HookConfiguration sintaks, lihat [Referensi sintaks skema konfigurasi hook](#).

Untuk menggunakan filter tingkat tumpukan, tambahkan StackFilters kunci di bawah HookConfiguration.

StackFiltersKuncinya memiliki satu anggota wajib dan memiliki dua anggota opsional.

- FilteringCriteria(Diperlukan)
- StackNames (opsional)
- StackRoles (opsional)

StackRolesProperti StackNames atau bersifat opsional. Namun, Anda harus menentukan setidaknya satu dari properti ini.

Jika Anda membuat Hook yang menargetkan operasi [Cloud Control API](#), semua filter tingkat tumpukan akan diabaikan.

FilteringCriteria

`FilteringCriteria` adalah parameter wajib yang menentukan perilaku penyaringan. Itu dapat diatur ke salah satu `ALL` atau `ANY`.

- `ALL` memanggil Hook jika semua filter cocok.
- `ANY` memanggil Hook jika ada satu filter yang cocok.

StackNames

Untuk menentukan satu atau beberapa nama tumpukan sebagai filter dalam konfigurasi Hooks Anda, gunakan struktur JSON berikut:

```
"StackNames": {
  "Include": [
    "string"
  ],
  "Exclude": [
    "string"
  ]
}
```

Anda harus menentukan salah satu dari berikut ini:

- `Include`: Daftar nama tumpukan untuk disertakan. Hanya tumpukan yang ditentukan dalam daftar ini yang akan memanggil Hook.
 - Tipe: Array string
 - Maks item: 50
 - Item min: 1
- `Exclude`: Daftar nama tumpukan untuk dikecualikan. Semua tumpukan kecuali yang tercantum di sini akan memanggil Hook.
 - Tipe: Array string
 - Maks item: 50
 - Item min: 1

Setiap nama tumpukan dalam `Include` dan `Exclude` array harus mematuhi pola dan persyaratan panjang berikut:

- Pola: `^[a-zA-Z][-a-zA-Z0-9]*$`
- Panjang maks: 128

`StackNames` mendukung nama tumpukan beton dan pencocokan wildcard lengkap. Untuk melihat contoh menggunakan wildcard, lihat [Menggunakan wildcard dengan nama target Hook](#).

StackRoles

Untuk menentukan satu atau beberapa [peran IAM](#) sebagai filter dalam konfigurasi Hook Anda, gunakan struktur JSON berikut:

```
"StackRoles": {
  "Include": [
    "string"
  ],
  "Exclude": [
    "string"
  ]
}
```

Anda harus menentukan salah satu dari berikut ini:

- `Include`: Daftar peran IAM ARNs untuk menargetkan tumpukan yang terkait dengan peran ini. Hanya operasi tumpukan yang diprakarsai oleh peran ini yang akan memanggil Hook.
 - Tipe: Array string
 - Maks item: 50
 - Item min: 1
- `Exclude`: Daftar peran IAM ARNs untuk tumpukan yang ingin Anda kecualikan. Hook akan dipanggil pada semua tumpukan kecuali yang diprakarsai oleh peran yang ditentukan.
 - Tipe: Array string
 - Maks item: 50
 - Item min: 1

Setiap peran tumpukan dalam `Include` dan `Exclude` array harus mematuhi pola dan persyaratan panjang berikut:

- Pola: `arn:.*:iam::[0-9]{12}:role/.+`
- Panjang maks: 256

`StackRoles`izinkan karakter wildcard di bagian sintaks [ARN](#) berikut:

- `partition`
- `account-id`
- `resource-id`

Untuk melihat contoh menggunakan wildcard di bagian sintaks ARN, lihat. [Menggunakan wildcard dengan nama target Hook](#)

Include dan Exclude

Setiap filter (`StackNames` dan `StackRoles`) memiliki `Include` daftar dan `Exclude` daftar. Menggunakan `StackNames` sebagai contoh, Hook hanya dipanggil pada tumpukan yang ditentukan dalam `Include` daftar. Jika nama tumpukan hanya ditentukan dalam `Exclude` daftar, hook hanya dipanggil pada tumpukan yang tidak ada dalam daftar. `Exclude` Jika keduanya `Include` dan `Exclude` ditentukan, Hook menargetkan apa yang ada dalam `Include` daftar dan bukan apa yang ada dalam `Exclude` daftar.

Misalnya, Anda memiliki empat tumpukan: A, B, C, dan D.

- `"Include": ["A", "B"]` Hook dipanggil pada A dan B.
- `"Exclude": ["B"]` Hook dipanggil pada A, C, dan D.
- `"Include": ["A", "B", "C"], "Exclude": ["A", "D"]` Hook dipanggil pada B dan C.
- `"Include": ["A", "B", "C"], "Exclude": ["A", "B", "C"]` Hook tidak dipanggil pada tumpukan apa pun.

Contoh filter tingkat tumpukan

Bagian ini memberikan contoh yang dapat Anda ikuti untuk membuat filter tingkat tumpukan untuk CloudFormation Hooks.

Contoh 1: Sertakan tumpukan tertentu

Contoh berikut menentukan Include daftar. Hook hanya dipanggil pada tumpukan bernama `stack-test-1`, `stack-test-2` dan `stack-test-3`

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Include": [
            "stack-test-1",
            "stack-test-2",
            "stack-test-3"
          ]
        }
      }
    }
  }
}
```

Contoh 2: Kecualikan tumpukan tertentu

Jika nama tumpukan ditambahkan ke Exclude daftar, Hook dipanggil pada tumpukan apa pun yang tidak diberi nama `stack-test-1`, `stack-test-2` atau `stack-test-3`.

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],

```

```

"FailureMode": "WARN",
"Properties": {},
"StackFilters": {
  "FilteringCriteria": "ALL",
  "StackNames": {
    "Exclude": [
      "stack-test-1",
      "stack-test-2",
      "stack-test-3"
    ]
  }
}
}
}
}
}

```

Contoh 3: Menggabungkan include dan exclude

Jika Include dan Exclude daftar tidak ditentukan, Hook hanya dipanggil pada tumpukan di Include yang tidak ada dalam daftar. Exclude Dalam contoh berikut, Hook hanya dipanggil pada stack-test-3.

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Include": [
            "stack-test-1",
            "stack-test-2",
            "stack-test-3"
          ],
          "Exclude": [
            "stack-test-1",
            "stack-test-2"
          ]
        }
      }
    }
  }
}

```


Contoh 5: Menggabungkan nama tumpukan dan peran dengan **ANY** kriteria

Hook berikut mencakup tiga nama tumpukan, dan satu peran tumpukan. Karena *FilteringCriteria* ditentukan sebagai **ANY**, Hook dipanggil untuk tumpukan yang memiliki nama tumpukan yang cocok atau peran tumpukan yang cocok.

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ANY",
        "StackNames": {
          "Include": [
            "stack-test-1",
            "stack-test-2",
            "stack-test-3"
          ]
        }
      },
      "StackRoles": {
        "Include": ["arn:aws:iam::123456789012:role/hook-role"]
      }
    }
  }
}
```

CloudFormation Filter target kait

Topik ini memberikan panduan tentang mengonfigurasi filter target untuk CloudFormation Hooks. Anda dapat menggunakan filter target untuk kontrol yang lebih terperinci atas kapan dan sumber daya mana Hook Anda dipanggil. Anda dapat mengonfigurasi filter mulai dari penargetan tipe sumber daya sederhana hingga kombinasi jenis sumber daya, tindakan, dan titik pemanggilan yang lebih kompleks.

Untuk menentukan satu atau beberapa nama tumpukan sebagai filter dalam konfigurasi Hooks Anda, tambahkan `TargetFilters` kunci di `bawahHookConfiguration`.

`TargetFilters` mendukung properti berikut.

Actions

Sebuah array string yang menentukan tindakan untuk menargetkan. Sebagai contoh, lihat [Contoh 1: Filter target dasar](#).

Nilai yang valid: CREATE | UPDATE | DELETE

Note

Untuk `RESOURCE`, `STACK`, dan `CLOUD_CONTROL` target, semua tindakan target dapat diterapkan. Untuk `CHANGE_SET` target, hanya CREATE tindakan yang berlaku. Untuk informasi selengkapnya, lihat [Target kait](#).

InvocationPoints

Sebuah array string yang menentukan titik pemanggilan ke target.

Nilai yang valid: PRE_PROVISION

TargetNames

Sebuah array string yang menentukan nama jenis sumber daya untuk menargetkan, misalnya, `AWS::S3::Bucket`.

Nama target mendukung nama target konkret dan pencocokan wildcard lengkap. Untuk informasi selengkapnya, lihat [Menggunakan wildcard dengan nama target Hook](#).

Pola: `^[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}::[a-zA-Z0-9]{2,64}$`

Maksimum: 50

Targets

Sebuah array objek yang menentukan daftar target yang akan digunakan untuk target pemfilteran.

Setiap target dalam array target memiliki properti berikut.

Actions

Tindakan untuk target yang ditentukan.

Nilai yang valid: CREATE | UPDATE | DELETE

InvocationPoints

Titik pemanggilan untuk target yang ditentukan.

Nilai yang valid: PRE_PROVISION

TargetNames

Nama jenis sumber daya untuk ditargetkan.

Note

Anda tidak dapat menyertakan array `Targets` objek dan `TargetNames`, `Actions`, atau `InvocationPoints` array pada saat yang sama. Jika Anda ingin menggunakan ketiga item ini dan `Targets`, Anda harus memasukkannya ke dalam array `Targets` objek. Sebagai contoh, lihat [Contoh 2: Menggunakan array Targets objek](#).

Contoh filter target

Bagian ini memberikan contoh yang dapat Anda ikuti untuk membuat filter target untuk CloudFormation Hooks.

Contoh 1: Filter target dasar

Untuk membuat filter target dasar yang berfokus pada jenis sumber daya tertentu, gunakan `TargetFilters` objek dengan `Actions` array. Konfigurasi filter target berikut akan memanggil Hook pada semua `Create`, `Update`, dan `Delete` tindakan untuk operasi target yang ditentukan (dalam hal ini, keduanya `RESOURCE` dan `STACK` operasi).

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
```

```

    "RESOURCE"
  ],
  "FailureMode": "WARN",
  "Properties": {},
  "TargetFilters": {
    "Actions": [
      "Create",
      "Update",
      "Delete"
    ]
  }
}
}
}
}

```

Contoh 2: Menggunakan array **Targets** objek

Untuk filter yang lebih canggih, Anda dapat menggunakan array **Targets** objek untuk mencantumkan kombinasi target, tindakan, dan titik pemanggilan tertentu. Konfigurasi filter target berikut ini akan memanggil Hook sebelum CREATE dan UPDATE tindakan pada bucket S3 dan tabel DynamoDB. Ini berlaku untuk keduanya STACK dan RESOURCE operasi.

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "TargetFilters": {
        "Targets": [
          {
            "TargetName": "AWS::S3::Bucket",
            "Action": "CREATE",
            "InvocationPoint": "PRE_PROVISION"
          },
          {
            "TargetName": "AWS::S3::Bucket",
            "Action": "UPDATE",
            "InvocationPoint": "PRE_PROVISION"
          }
        ]
      }
    }
  }
}

```

```

    },
    {
      "TargetName": "AWS::DynamoDB::Table",
      "Action": "CREATE",
      "InvocationPoint": "PRE_PROVISION"
    },
    {
      "TargetName": "AWS::DynamoDB::Table",
      "Action": "UPDATE",
      "InvocationPoint": "PRE_PROVISION"
    }
  ]
}
}
}
}
}

```

Menggunakan wildcard dengan nama target Hook

Anda dapat menggunakan wildcard sebagai bagian dari nama target. Anda dapat menggunakan karakter wildcard (*dan?) dalam nama target Hook Anda. Tanda bintang (*) mewakili kombinasi karakter apa pun. Tanda tanya (?) mewakili setiap karakter tunggal. Anda dapat menggunakan beberapa * dan ? karakter dalam nama target.

Example: Contoh wildcard nama target dalam skema Hook

Contoh berikut menargetkan semua jenis sumber daya yang didukung oleh Amazon S3.

```

{
  ...
  "handlers": {
    "preCreate": {
      "targetNames": [
        "AWS::S3::*"
      ],
      "permissions": []
    }
  }
  ...
}

```

Contoh berikut cocok dengan semua jenis sumber daya yang memiliki Bucket "" dalam nama.

```
{
  ...
  "handlers": {
    "preCreate": {
      "targetNames": [
        "AWS::*::Bucket*"
      ],
      "permissions": []
    }
  }
  ...
}
```

`AWS::*::Bucket*` Mungkin menyelesaikan salah satu jenis sumber daya konkret berikut:

- `AWS::Lightsail::Bucket`
- `AWS::S3::Bucket`
- `AWS::S3::BucketPolicy`
- `AWS::S3Outpost::Bucket`
- `AWS::S3Outpost::BucketPolicy`

Example: Contoh wildcard nama target dalam skema konfigurasi Hook

Contoh konfigurasi berikut memanggil Hook untuk CREATE operasi pada semua jenis sumber daya Amazon S3, dan UPDATE untuk operasi pada semua jenis sumber daya tabel bernama, seperti `AWS::DynamoDB::Table` atau `AWS::Glue::Table`

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "TargetStacks": "ALL",
      "FailureMode": "FAIL",
      "Properties": {},
      "TargetFilters": {
        "Targets": [
          {
            "TargetName": "AWS::S3::*",
            "Action": "CREATE",
            "InvocationPoint": "PRE_PROVISION"
          }
        ]
      }
    }
  }
}
```



```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Include": [
            "stack-test-*"
          ]
        }
      }
    }
  }
}
```

Example: tumpukan Exclude khusus

Contoh berikut menentukan Exclude daftar. Hook dipanggil pada tumpukan apa pun yang tidak dimulaistack-test-.

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Exclude": [
            "stack-test-*"
          ]
        }
      }
    }
  }
}
```

```

    }
  }
}
}
}

```

Example: Menggabungkan Include dan Exclude untuk tumpukan tertentu

Jika Include dan Exclude daftar ditentukan, Hook hanya dipanggil pada tumpukan yang cocok dengan Include yang tidak cocok dalam daftar. Exclude Dalam contoh berikut, Hook dipanggil pada semua tumpukan yang dimulai dengan stack-test- kecuali untuk tumpukan bernama stack-test-1,, stack-test-2 dan. stack-test-3

```

{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackNames": {
          "Include": [
            "stack-test-*"
          ],
          "Exclude": [
            "stack-test-1",
            "stack-test-2",
            "stack-test-3"
          ]
        }
      }
    }
  }
}
}
}
}

```

Example: peran Include khusus

Contoh berikut menentukan Include daftar dengan dua pola wildcard. Entri pertama akan menjalankan Hook untuk peran apa pun yang dimulai dengan hook-role dalam setiap partition dan account-id. Entri kedua akan menjalankan apa pun untuk peran apa pun dalam apa pun partition yang dimiliki account-id123456789012.

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ALL",
        "StackRoles": {
          "Include": [
            "arn:*:iam:*:role/hook-role*",
            "arn:*:iam::123456789012:role/*"
          ]
        }
      }
    }
  }
}
```

Example: peran Exclude khusus

Contoh berikut menentukan Exclude daftar dengan dua pola wildcard. Entri pertama akan melewati eksekusi Hook ketika peran memiliki namanya exempt di setiap partition dan apa pun account-id. Entri kedua akan melewati eksekusi Hook ketika peran milik account-id 123456789012 digunakan dengan operasi tumpukan.

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
```


Example: Menggabungkan StackNames dan StackRoles dengan kriteria apa pun

Hook berikut mencakup satu wildcard nama stack dan satu wildcard peran stack. Karena `FilteringCriteria` ditentukan sebagai `ANY`, Hook dipanggil untuk tumpukan yang memiliki pencocokan `StackNames` atau pencocokan `StackRoles`.

```
{
  "CloudFormationConfiguration": {
    "HookConfiguration": {
      "HookInvocationStatus": "ENABLED",
      "TargetOperations": [
        "STACK",
        "RESOURCE"
      ],
      "FailureMode": "WARN",
      "Properties": {},
      "StackFilters": {
        "FilteringCriteria": "ANY",
        "StackNames": {
          "Include": [
            "stack-test-*"
          ]
        },
        "StackRoles": {
          "Include": ["arn:*:iam:*:*:role/hook-role*"]
        }
      }
    }
  }
}
```

Buat Hooks menggunakan template CloudFormation

Halaman ini menyediakan tautan ke CloudFormation templat sampel dan topik referensi teknis untuk Hooks.

Dengan menggunakan CloudFormation template untuk membuat Hooks, Anda dapat menggunakan kembali template Anda untuk mengatur Hooks Anda secara konsisten dan berulang kali. Pendekatan ini memungkinkan Anda untuk menentukan Hooks Anda sekali, dan kemudian menyediakan Hooks yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

CloudFormation menawarkan jenis sumber daya khusus berikut untuk pembuatan Guard dan Lambda Hook.

Tugas	Solusi	Tautan
Buat Guard Hook	Gunakan jenis <code>AWS::CloudFormation::GuardHook</code> sumber daya untuk membuat dan mengaktifkan Guard Hook.	Template sampel Referensi teknis
Buat Lambda Hook	Gunakan jenis <code>AWS::CloudFormation::LambdaHook</code> sumber daya untuk membuat dan mengaktifkan Lambda Hook.	Template sampel Referensi teknis

CloudFormation juga menawarkan jenis sumber daya berikut yang dapat Anda gunakan dalam template tumpukan Anda untuk pembuatan Hook kustom.

Tugas	Solusi	Tautan
Daftarkan Hook	Gunakan jenis <code>AWS::CloudFormation::HookVersion</code> sumber daya untuk menerbitkan versi baru atau pertama dari Hook kustom ke CloudFormation registri.	Contoh template Referensi teknis

Tugas	Solusi	Tautan
Mengatur konfigurasi Hook	Gunakan jenis <code>AWS::CloudFormation::HookTypeConfig</code> sumber daya untuk menentukan konfigurasi Hook kustom.	Contoh template Referensi teknis
Mengatur versi default Hook	Gunakan jenis <code>AWS::CloudFormation::HookDefaultVersion</code> sumber daya untuk menentukan versi default dari Hook kustom.	Contoh template Referensi teknis
Daftarkan akun Anda sebagai penerbit	Gunakan jenis <code>AWS::CloudFormation::Publisher</code> sumber daya untuk mendaftarkan akun Anda sebagai penerbit ekstensi publik (Hooks, modul, dan jenis sumber daya) di registri. CloudFormation	Referensi teknis
Publikasikan Hook secara publik	Gunakan jenis <code>AWS::CloudFormation::PublicTypeVersion</code> sumber daya untuk menguji dan menerbitkan Hook kustom terdaftar sebagai Hook pihak ketiga publik.	Referensi teknis
Aktifkan Hooks publik dan pihak ketiga	Jenis <code>AWS::CloudFormation::TypeActivation</code> sumber daya bekerja sama dengan jenis <code>AWS::CloudFormation::HookTypeConfig</code> sumber daya untuk mengaktifkan Hook kustom pihak ketiga publik di akun Anda.	Referensi teknis

Berikan izin IAM untuk Hooks CloudFormation

Secara default, pengguna baru di Akun AWS tidak memiliki izin untuk mengelola Hooks menggunakan Konsol Manajemen AWS, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Gunakan contoh kebijakan dalam topik ini untuk membuat kebijakan IAM kustom Anda sendiri guna memberikan izin kepada pengguna untuk bekerja dengan Hooks.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Menentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan di Panduan Pengguna IAM](#).

Topik ini mencakup izin yang diperlukan untuk melakukan hal berikut:

- Kelola Hooks — Buat, modifikasi, dan nonaktifkan Hooks di akun Anda.
- Publikasikan Hooks secara publik — Daftarkan, uji, dan publikasikan Hooks kustom Anda untuk membuatnya tersedia untuk umum di registri. CloudFormation
- Lihat hasil pemanggilan — Akses dan kueri hasil pemanggilan Hook di akun Anda.
- Lihat detail untuk hasil pemanggilan — Akses informasi terperinci dan panduan remediasi untuk hasil pemanggilan Hook tertentu di akun Anda.

Saat membuat kebijakan IAM, Anda dapat menemukan dokumentasi untuk semua tindakan, sumber daya, dan kunci kondisi yang terkait dengan awalan `cloudformation` layanan di [kunci Tindakan, sumber daya, dan kondisi untuk CloudFormation](#) bagian Referensi Otorisasi Layanan.

Topik

- [Izinkan pengguna untuk mengelola Hooks](#)
- [Izinkan pengguna untuk mempublikasikan Hooks kustom secara publik](#)
- [Izinkan pengguna untuk melihat hasil pemanggilan Hook](#)
- [Izinkan pengguna untuk melihat hasil pemanggilan Hook yang terperinci](#)
- [AWS KMS kebijakan kunci dan izin untuk mengenkripsi hasil CloudFormation Hooks saat istirahat](#)

Izinkan pengguna untuk mengelola Hooks

Jika Anda perlu mengizinkan pengguna untuk mengelola ekstensi, termasuk Hooks, tanpa kemampuan untuk membuatnya publik di CloudFormation registri, Anda dapat menggunakan contoh berikut kebijakan IAM.

Important

Panggilan `SetTypeConfiguration` API `ActivateType` dan bekerja sama untuk membuat Hooks di akun Anda. Saat Anda memberikan izin kepada pengguna untuk memanggil `SetTypeConfiguration` API, Anda secara otomatis memberi mereka kemampuan untuk memodifikasi dan menonaktifkan Hooks yang ada. Anda tidak dapat menggunakan izin tingkat sumber daya untuk membatasi akses ke panggilan API ini. Oleh karena itu, pastikan bahwa Anda memberikan izin ini hanya kepada pengguna yang berwenang di akun Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:ActivateType",
        "cloudformation:DescribeType",
        "cloudformation:ListTypes",
        "cloudformation:SetTypeConfiguration"
      ],
      "Resource": "*"
    }
  ]
}
```

Pengguna yang mengelola Hooks mungkin memerlukan beberapa izin terkait, misalnya:

- Untuk melihat kontrol proaktif dari Katalog Kontrol di CloudFormation konsol, pengguna harus memiliki `controlcatalog:ListControls` izin dalam kebijakan IAM.

- Untuk mendaftarkan Hooks kustom sebagai ekstensi pribadi di CloudFormation registri, pengguna harus memiliki `cloudformation:RegisterType` izin dalam kebijakan IAM.

Izinkan pengguna untuk mempublikasikan Hooks kustom secara publik

Contoh berikut kebijakan IAM berfokus secara khusus pada kemampuan penerbitan. Gunakan kebijakan ini jika Anda perlu mengizinkan pengguna membuat ekstensi, termasuk Hooks, tersedia untuk umum di registri. CloudFormation

Important

Publishing Hooks secara publik membuatnya tersedia untuk orang lain. Akun AWS Pastikan bahwa hanya pengguna yang berwenang yang memiliki izin ini dan ekstensi yang dipublikasikan memenuhi standar kualitas dan keamanan organisasi Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeTypeRegistration",
        "cloudformation:ListTypes",
        "cloudformation:ListTypeVersions",
        "cloudformation:PublishType",
        "cloudformation:RegisterPublisher",
        "cloudformation:RegisterType",
        "cloudformation:TestType"
      ],
      "Resource": "*"
    }
  ]
}
```

Izinkan pengguna untuk melihat hasil pemanggilan Hook

Izin IAM yang diperlukan untuk melihat hasil pemanggilan Hook berubah tergantung pada jenis informasi yang diminta.

Daftar hasil pemanggilan Hook

Untuk mencantumkan hasil pemanggilan Hook, pengguna memerlukan izin yang berbeda tergantung pada permintaan API yang dibuat.

- Untuk memberikan izin untuk meminta semua hasil Hook, hasil untuk Hook tertentu, atau hasil untuk status Hook dan pemanggilan tertentu, Anda harus memberikan akses ke tindakan tersebut. `cloudformation:ListAllHookResults`
- Untuk memberikan izin untuk meminta hasil dengan menentukan target Hook, Anda harus memberikan akses ke tindakan. `cloudformation:ListHookResults` Izin ini memungkinkan pemanggil API untuk menentukan `TargetType` dan `TargetId` parameter saat memanggil `ListHookResults`.

Berikut ini menunjukkan contoh kebijakan izin dasar untuk mencantumkan hasil pemanggilan Hook. Identitas IAM (pengguna atau peran) dengan kebijakan ini memiliki izin untuk meminta semua hasil pemanggilan menggunakan semua kombinasi parameter yang tersedia.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:ListAllHookResults",
        "cloudformation:ListHookResults"
      ],
      "Resource": "*"
    }
  ]
}
```

Kontrol set perubahan mana yang dapat ditentukan

Contoh berikut kebijakan IAM memberikan izin untuk `cloudformation:ListHookResults` tindakan untuk meminta hasil dengan menentukan target Hook. Namun, itu juga menyangkal tindakan jika target adalah set perubahan bernama `example-changeset`.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:ListHookResults"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:ListHookResults"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudformation:ChangeSetName": "example-changeset"
        }
      }
    }
  ]
}
```

Kontrol Hooks mana yang dapat ditentukan

Contoh berikut kebijakan IAM memberikan izin untuk `cloudformation:ListAllHookResults` tindakan untuk meminta hasil pemanggilan hanya jika ARN Hook disediakan dalam permintaan. Ini menyangkal tindakan untuk Hook ARN tertentu.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:ListAllHookResults"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:ListAllHookResults"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:TypeArn": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:ListAllHookResults"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "cloudformation:TypeArn": "arn:aws:cloudformation:us-
east-1:123456789012:type/hook/MyCompany-MyHook"
        }
      }
    }
  ]
}
```

Izinkan pengguna untuk melihat hasil pemanggilan Hook yang terperinci

Untuk memberikan izin untuk melihat hasil rinci dari pemanggilan Hook tertentu, Anda harus memberikan akses ke tindakan tersebut. `cloudformation:GetHookResult` Izin ini memungkinkan pengguna untuk mengambil informasi rinci dan panduan remediasi untuk hasil pemanggilan Hook tertentu. Untuk informasi selengkapnya, lihat [GetHookResult](#) di dalam Referensi API AWS CloudFormation .

Contoh berikut kebijakan IAM memberikan izin untuk tindakan tersebut.

```
cloudformation:GetHookResult
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetHookResult"
      ],
      "Resource": "*"
    }
  ]
}
```

Note

Anda dapat mengonfigurasi Hooks untuk mengenkripsi hasil pemanggilan terperinci yang disimpan di cloud dengan kunci Anda sendiri. AWS KMS Untuk informasi tentang cara menyiapkan kebijakan kunci dan izin IAM yang Anda perlukan saat menggunakan kunci terkelola pelanggan untuk enkripsi, lihat. [AWS KMS kebijakan kunci dan izin untuk mengenkripsi hasil CloudFormation Hooks saat istirahat](#)

AWS KMS kebijakan kunci dan izin untuk mengenkripsi hasil CloudFormation Hooks saat istirahat

Topik ini menjelaskan cara menyiapkan kebijakan AWS KMS kunci dan izin yang Anda perlukan saat menentukan kunci terkelola pelanggan untuk mengenkripsi data anotasi Hooks yang tersedia dari API. [GetHookResult](#)

Note

CloudFormation Hooks tidak memerlukan otorisasi tambahan untuk menggunakan default Kunci milik AWS untuk mengenkripsi data anotasi di akun Anda.

Topik

- [Ikhtisar](#)
- [Menggunakan konteks enkripsi untuk mengontrol akses ke kunci terkelola pelanggan Anda](#)
- [Kebijakan kunci KMS yang dikelola pelanggan](#)
- [Izin KMS untuk API SetTypeConfiguration](#)
- [Izin KMS untuk API GetHookResult](#)

Ikhtisar

Berikut ini AWS KMS keys dapat digunakan untuk mengenkripsi data anotasi Hook:

- [Kunci milik AWS](#)— Secara default, CloudFormation menggunakan Kunci milik AWS untuk mengenkripsi data. Anda tidak dapat melihat, mengelola, atau menggunakan Kunci milik AWS, atau mengaudit penggunaannya. Namun, Anda tidak perlu melakukan konfigurasi eksplisit untuk melindungi kunci yang digunakan untuk mengenkripsi data Anda. Kunci milik AWS disediakan secara gratis (tidak ada biaya bulanan atau biaya penggunaan). Kecuali Anda diminta untuk mengaudit atau mengontrol kunci enkripsi yang melindungi data anotasi Anda, a Kunci milik AWS adalah pilihan yang baik.
- [Kunci terkelola pelanggan](#) — CloudFormation mendukung penggunaan kunci terkelola pelanggan simetris yang Anda buat, miliki, dan kelola untuk menambahkan lapisan enkripsi kedua di atas yang ada Kunci milik AWS. AWS KMS dikenakan biaya. Untuk informasi selengkapnya, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengembang. Untuk mengelola kunci

Anda, gunakan AWS Key Management Service (AWS KMS) di [AWS KMS konsol](#), the AWS CLI, atau AWS KMS API. Lihat informasi selengkapnya di [Panduan Developer AWS Key Management Service](#).

Anda dapat mengonfigurasi kunci yang dikelola pelanggan saat membuat dan memperbarui Hooks. Saat Anda memberikan kunci terkelola pelanggan Anda, CloudFormation gunakan kunci ini untuk mengenkripsi data anotasi sebelum menyimpannya. Ketika data anotasi kemudian diakses selama operasi `GetHookResult` API, CloudFormation secara otomatis mendekripsi data tersebut. Untuk informasi tentang mengonfigurasi kunci enkripsi untuk Hooks, lihat [Referensi sintaks skema konfigurasi hook](#)

Important

Perhatikan bahwa `KmsKeyId` opsi untuk menentukan kunci yang dikelola pelanggan saat ini hanya tersedia saat Anda menggunakan tombol AWS CLI untuk mengonfigurasi Hook Anda.

Menggunakan konteks enkripsi untuk mengontrol akses ke kunci terkelola pelanggan Anda

CloudFormation Hooks secara otomatis menyertakan konteks enkripsi dengan setiap penyimpanan anotasi dan operasi pengambilan. Ini memungkinkan Anda menyetel kondisi konteks enkripsi dalam kebijakan kunci untuk memastikan kunci hanya dapat digunakan untuk Hook tertentu:

- `kms:EncryptionContext:aws:cloudformation:hooks:service`— Memastikan kunci hanya digunakan oleh layanan CloudFormation Hooks.
- `kms:EncryptionContext:aws:cloudformation:account-id`— Mencegah penggunaan kunci lintas akun dengan mencocokkan Akun AWS ID Anda.
- `kms:EncryptionContext:aws:cloudformation:arn`— Batasi penggunaan untuk Hooks tertentu menggunakan pola ARN.

Kondisi ini memberikan perlindungan tambahan terhadap serangan wakil yang membingungkan dengan mengikat data terenkripsi secara kriptografis ke konteks Hook tertentu.

Kebijakan kunci KMS yang dikelola pelanggan

Saat membuat kunci terkelola pelanggan Anda, Anda harus menentukan kebijakan utamanya untuk memungkinkan layanan CloudFormation Hooks melakukan AWS KMS operasi. Untuk menggunakan kebijakan kunci berikut, ganti *placeholder values* dengan informasi Anda sendiri.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnableIAMUserDescribeKey",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/ExampleRole"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "cloudformation.us-east-1.amazonaws.com"
        }
      }
    },
    {
      "Sid": "EnableIAMUserGenerateDataKey",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/ExampleRole"
      },
      "Action": "kms:GenerateDataKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "cloudformation.us-east-1.amazonaws.com",
          "kms:EncryptionContext:aws:cloudformation:hooks:service":
            "hooks.cloudformation.amazonaws.com",
          "kms:EncryptionContext:aws:cloudformation:123456789012": "123456789012"
        }
      },
      "ArnLike": {

```

```

    "kms:EncryptionContext:aws:cloudformation:arn":
"arn:aws:cloudformation:*:123456789012:hook/*"
  }
}
},
{
  "Sid": "EnableIAMUserDecrypt",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:role/ExampleRole"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "cloudformation.us-east-1.amazonaws.com"
    }
  }
},
{
  "Sid": "AllowHooksServiceDescribeKey",
  "Effect": "Allow",
  "Principal": {
    "Service": "hooks.cloudformation.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012"
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:cloudformation:*:123456789012:hook/*"
    }
  }
},
{
  "Sid": "AllowHooksService",
  "Effect": "Allow",
  "Principal": {
    "Service": "hooks.cloudformation.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",

```

```

    "kms:GenerateDataKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "123456789012",
      "kms:EncryptionContext:aws:cloudformation:hooks:service":
"hooks.cloudformation.amazonaws.com",
      "kms:EncryptionContext:aws:cloudformation:123456789012": "123456789012"
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:cloudformation:*:123456789012:hook/*",
      "kms:EncryptionContext:aws:cloudformation:arn":
"arn:aws:cloudformation:*:123456789012:hook/*"
    }
  }
}
]
}

```

Kebijakan ini memberikan izin untuk peran IAM (tiga pernyataan pertama) dan layanan CloudFormation Hooks (dua pernyataan terakhir). Kunci `kms:ViaService` kondisi memastikan kunci KMS hanya dapat digunakan CloudFormation, mencegah panggilan API KMS langsung. Operasi kuncinya adalah:

- `kms:DescribeKey`— Memvalidasi properti utama dan metadata. Operasi ini dalam pernyataan terpisah karena tidak dapat digunakan dengan kondisi konteks enkripsi.
- `kms:GenerateDataKey`— Menghasilkan kunci enkripsi data untuk mengenkripsi anotasi sebelum penyimpanan. Operasi ini mencakup kondisi konteks enkripsi untuk kontrol akses cakupan.
- `kms:Decrypt`— Mendekripsi data anotasi yang sebelumnya dienkripsi. Untuk peran IAM, ini termasuk `kms:ViaService` kondisi. Untuk prinsipal layanan, ini termasuk kondisi konteks enkripsi.

Kunci `aws:SourceAccount` dan `aws:SourceArn` kondisi memberikan perlindungan utama terhadap serangan wakil yang membingungkan. Kondisi konteks enkripsi menyediakan lapisan validasi tambahan. Untuk informasi selengkapnya, lihat [Menggunakan aws:SourceArn atau aws:SourceAccount mengkondisikan kunci](#) di Panduan AWS Key Management Service Pengembang.

⚠ Important

Peran eksekusi hook tidak memerlukan AWS KMS izin. Prinsipal layanan CloudFormation Hooks melakukan semua AWS KMS operasi.

Izin KMS untuk API **SetTypeConfiguration**

Selama panggilan [SetTypeConfiguration](#) API, CloudFormation memvalidasi izin pengguna untuk mengenkripsi data anotasi dengan kunci yang ditentukan. AWS KMS Tambahkan kebijakan IAM berikut ke pengguna atau peran yang akan mengonfigurasi enkripsi menggunakan SetTypeConfiguration API. Ganti *placeholder values* dengan informasi Anda sendiri.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudformation:SetTypeConfiguration",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "kms:DescribeKey",
      "Resource": "arn:aws:kms:us-east-1:123456789012:key/abc-123"
    },
    {
      "Effect": "Allow",
      "Action": "kms:GenerateDataKey",
      "Resource": "arn:aws:kms:us-east-1:123456789012:key/abc-123",
      "Condition": {
        "StringEquals": {
          "kms:EncryptionContext:aws:cloudformation:hooks:service":
            "hooks.cloudformation.amazonaws.com",
          "kms:EncryptionContext:aws:cloudformation:123456789012": "123456789012"
        },
        "ArnLike": {
          "kms:EncryptionContext:aws:cloudformation:arn":
            "arn:aws:cloudformation:*:123456789012:hook/*"
        }
      }
    }
  ]
}
```

```
    }
  }
]
}
```

Izin KMS untuk API `GetHookResult`

[GetHookResult](#) Untuk memanggil Hooks yang menggunakan kunci terkelola pelanggan Anda, pengguna harus memiliki `kms:Decrypt` izin untuk kunci tersebut. Tambahkan kebijakan IAM berikut ke pengguna atau peran yang akan memanggil `GetHookResult`. Ganti `arn:aws:kms:us-east-1:123456789012:key/abc-123` dengan ARN kunci yang dikelola pelanggan Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudformation:GetHookResult",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-east-1:123456789012:key/abc-123"
    }
  ]
}
```

Riwayat dokumen untuk panduan pengguna CloudFormation Hooks

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir CloudFormation Hooks. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

- Pembaruan dokumentasi terbaru: 4 September 2025.

Perubahan	Deskripsi	Tanggal
Hasil pemeriksaan kepatuhan terperinci	Hooks sekarang mendukung anotasi yang memberikan hasil pemeriksaan kepatuhan terperinci dan panduan remediasi untuk setiap sumber daya yang dievaluasi. Lihat hasil validasi terperinci ini melalui perintah CloudFormation konsol atau <code>get-hook-result</code> CLI.	November 13, 2025
Kontrol proaktif sebagai Hooks	Anda sekarang dapat mengaktifkan Hooks berbasis kontrol proaktif melalui konsol CloudFormation atau CLI menggunakan perintah <code>and.activate-type set-type-configuration</code> . Anda dapat mengonfigurasi Hooks ini untuk menerapkan AWS Control Tower kontrol proaktif Katalog Kontrol tertentu untuk mengevaluasi	September 4, 2025

sumber daya selama CREATE dan UPDATE operasi.

[Ringkasan pemanggilan kait](#)

Anda sekarang dapat mengambil informasi tentang pemanggilan Hook melalui CloudFormation konsol, atau menggunakan perintah `list-hook-results` CLI untuk mengambil detail pemanggilan secara terprogram. Anda juga sekarang dapat memfilter `list-hook-results` hasil berdasarkan status Hook atau pemanggilan untuk fokus pada pemanggilan yang relevan.

September 4, 2025

[Kait tingkat tumpukan](#)

Hooks sekarang didukung di tingkat tumpukan, memungkinkan pelanggan untuk menggunakan CloudFormation Hooks untuk mengevaluasi template baru dan berpotensi memblokir operasi tumpukan dari proses.

November 13, 2024

[AWS Cloud Control API](#) [Integrasi kait](#)

Hooks sekarang terintegrasi dengan Cloud Control API, memungkinkan pelanggan untuk menggunakan CloudFormation Hooks untuk secara proaktif memeriksa konfigurasi sumber daya sebelum penyediaan. Jika sumber daya yang tidak sesuai ditemukan, Hook akan gagal dalam operasi dan mencegah sumber daya disediakan, atau mengeluarkan peringatan dan memungkinkan operasi penyediaan dilanjutkan.

November 13, 2024

[AWS CloudFormation Guard](#) [Kait](#)

AWS CloudFormation Guard adalah bahasa khusus domain open-source dan tujuan umum (DSL) yang dapat Anda gunakan untuk menulis. policy-as-code Guard Hooks dapat mengevaluasi Cloud Control API dan CloudFormation operasi untuk memeriksa konfigurasi sumber daya sebelum penyediaan. Jika sumber daya yang tidak sesuai ditemukan, Hook akan gagal dalam operasi dan mencegah sumber daya disediakan, atau mengeluarkan peringatan dan memungkinkan operasi penyediaan dilanjutkan.

November 13, 2024

[AWS Lambda Kait](#)

AWS CloudFormation Lambda Hooks November 13, 2024

Hooks memungkinkan Anda untuk mengevaluasi CloudFormation dan operasi Cloud Control API terhadap kustom kode kustom Anda sendiri. Hook Anda dapat memblokir operasi agar tidak berjalan, atau mengeluarkan peringatan kepada penelepon dan memungkinkan operasi dilanjutkan.

[Panduan Pengguna Hooks](#)

Versi awal Panduan Pengguna CloudFormation Hooks 8 Desember 2023

Pembaruan mencakup pengenalan baru, panduan memulai, konsep dan terminologi, pemfilteran tingkat tumpukan, dan topik yang diperbarui tentang prasyarat, penyiapan, dan pengembangan Hooks. CloudFormation

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.